2020-09

EFFECTIVENESS OF NATIONAL CYBER POLICY TO STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS

Simon, Ian G.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EFFECTIVENESS OF NATIONAL CYBER POLICY TO STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS

by

Ian G. Simon

September 2020

Thesis Advisor:	Duane T. Davis
Second Reader:	Robert Bebber, IWTC Corry Station

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
EFFECTIVENESS OF NATIONAL CYBER POLICY TO STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS

5. FUNDING NUMBERS

6. AUTHOR(S) Ian G. Simon

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, directs a whole-of-government approach to strengthening the security and resilience of critical infrastructure against physical and cyber threats. Per policy, critical infrastructure is categorized into 16 sectors. Security and resiliency efforts against cyber threats are constrained by this sector-based approach. This thesis assesses the sector-based approach by the following criteria: expertise or a notable advantage of the sector-specific agency; promotion of cybersecurity measures by the critical infrastructure community partnership structure; and legislation, policy, or sector-specific characteristics that enhance security and resilience of the sector. These assessments gauged the adequacy of organizational structures that lead and support critical infrastructure cybersecurity.

Exemplar cyber attacks against critical infrastructure and response actions are described in order to demonstrate strengths and limitations of the sector-based approach. This examination reveals that the U.S. approach to critical infrastructure is well conceived and executed in general. A number of significant vulnerabilities do remain in some sectors, however, as a result of incomplete or insufficient implementation.

14. SUBJECT TERMS critical infrastructure, cyber, policy	**15. NUMBER OF PAGES** 93
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

EFFECTIVENESS OF NATIONAL CYBER POLICY TO STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS

Ian G. Simon
Lieutenant Commander, United States Navy
BS, U.S. Naval Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2020

Approved by: Duane T. Davis
Advisor

Robert Bebber
Second Reader

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, directs a whole-of-government approach to strengthening the security and resilience of critical infrastructure against physical and cyber threats. Per policy, critical infrastructure is categorized into 16 sectors. Security and resiliency efforts against cyber threats are constrained by this sector-based approach. This thesis assesses the sector-based approach by the following criteria: expertise or a notable advantage of the sector-specific agency; promotion of cybersecurity measures by the critical infrastructure community partnership structure; and legislation, policy, or sector-specific characteristics that enhance security and resilience of the sector. These assessments gauged the adequacy of organizational structures that lead and support critical infrastructure cybersecurity.

Exemplar cyber attacks against critical infrastructure and response actions are described in order to demonstrate strengths and limitations of the sector-based approach. This examination reveals that the U.S. approach to critical infrastructure is well conceived and executed in general. A number of significant vulnerabilities do remain in some sectors, however, as a result of incomplete or insufficient implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CFATS	Chemical Facilities Anti-Terrorism Standards
CIKR	critical infrastructure and key resources
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CS&C	Office of Cybersecurity and Communications
DDoS	distributed denial of service
DIB	Defense Industrial Base
DHS	Department of Homeland Security
DNS	Domain Name System
DOD	Department of Defense
DoE	Department of Energy
DoJ	Department of Justice
DoT	Department of Transportation
EPA	Environmental Protection Agency
FCC	Federal Communications Commission
FDA	Food and Drug Administration
GAO	Government Accountability Office
GSA	Government Services Administration
HSIN	Homeland Security Information Network
HHS	Department of Health and Human Services
HVAC	heating, ventilation, and air conditioning
ICS	industrial control system
ICS-CERT	Industrial Control System Cyber Emergency Response Team
ISAC	Information Sharing and Analysis Center
IT	information technology
NCIPP	National Critical Infrastructure Protection Plan
NCIJTF	National Cyber Investigative Joint Task Force
NCCIC	National Cybersecurity and Communications Integration Center
NIPP	National Infrastructure Protection Plan

NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
NRC	Nuclear Regulatory Commission
NRMC	National Risk Management Center
NSA	National Security Agency
PPD	Presidential Policy Directive
SCADA	supervisory and data acquisition
US-CERT	United States Computer Emergency Response Team
USC	United States Code
USDA	US Department of Agriculture

I. INTRODUCTION

A. OVERVIEW AND MOTIVATION

The U.S. government has established 16 sectors of critical infrastructure that are essential to the functioning of the nation. As stated in Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, "It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats" [1]. PPD-21 defines critical infrastructure, outlines why government needs to focus its resources on protecting each sector, and establishes roles and responsibilities for various government entities.

PPD-21 assigns the Department of Homeland Security (DHS) as the lead agency for protection of critical infrastructure, and as the entity with primacy of the assigned task DHS is required to "provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure" [1]. The sector-based approach to critical infrastructure constrains efforts to implement cybersecurity measures.

To date, however, the overall efficacy of the sector-based approach as prescribed by PPD-21 has not been fully assessed and there is no qualitative measure of the efficacy of the sector-based approach. Example cyber attacks against U.S. critical structure are examined in the context of PPD-21 in order to assess the organizational response to cyber incidents.

With PPD-21 as a starting point, this research examines U.S. policies and organizations that pertain to the cyber aspects of critical infrastructure security and resilience in order to gauge whether or not critical infrastructure sectors are appropriately aligned to carry out the task. When examining the cyber aspects of critical infrastructure, U.S. policies and organizations, and incident response actions, PPD-41, United States Cyber Incident Coordination, was an additional starting point. PPD-41 provides an initial alignment of U.S. government organizations with roles and responsibilities identified, for response and follow-on actions to a cyber incident [2].

B. CRITICAL INFRASTRUCTURE OVERVIEW

PPD-21 and PPD-41 provide definitions and terms that are carried forward in subsequent policy documents and that are used by U.S. government agencies with critical infrastructure protection roles and responsibilities. These policy directives provide descriptions of what is classified as critical infrastructure, what is meant by security and resilience, and what qualifies as a cyber incident in the context of U.S. government policy.

In particular, PPD-21 identifies 16 critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" [1]. These assets, systems, and networks span the nation physically and encompass significant portions of the economy and infrastructure. Further, these sectors are not necessarily discrete and are often interconnected or interdependent. Each critical infrastructure sector is assigned a corresponding sector-specific agency with primary responsibility for implementation of PPD-21 requirements for that sector.

A sector-specific agency is a federal agency or department assigned roles and responsibilities for a sector of critical infrastructure. Assignment is typically based on a combination of preexisting statutory or regulatory authorities and presumed knowledge and expertise of the respective sector and its characteristics. The roles and responsibilities of the sector-specific agencies include acting as the primary interface between DHS, other federal entities, and the owners and operators of the respective sector's critical infrastructure; leading day-to-day efforts with federal involvement; executing incident management responsibilities; and providing general support to the sectors.

The sector-specific agencies are broadly responsible for ensuring resilience of their respective sectors, while owners and operators of critical infrastructure are primarily responsible for security. Resilience is defined as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions [including] the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents" [1]. Security, on the other hand, is defined as "reducing the risk to

critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters" [1].

PPD-41 describes a cyber incident as an event or vulnerability that affects the confidentiality, integrity, or availability of information of an information system, and goes further in defining a significant cyber incident as an incident that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people" [2]. Drawing from this definition, it is reasonable to generalize that cyber attacks against critical infrastructure have the potential to escalate into significant cyber incidents.

PPD-21 and PPD-41 provide explicit and implicit tasking. These directives also lay out coordination efforts, reporting requirements, and basic strategies. The entities used for incident response, as defined in PPD-41, align with those identified in PPD-21.

C. ORDERS, TASKS, AND ROLES & RESPONSIBILITIES

The following strategic PPD-21 imperatives dictate the federal effort to strengthen the security and resilience of critical infrastructure [1]:

> Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
>
> Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
>
> Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

In the context of cyber incidents, these imperatives are subsumed by three concurrent lines of effort defined in PPD-41 for government response to a cyber incident: threat response, asset response, and intelligence support and related activities. An additional line of effort is required if a federal agency is affected by the cyber incident; specifically, mitigation of the effects to the agency.

Threat response activities are efforts to identify cyber attack perpetrators and bring them to justice. These activities are led by the Department of Justice (DoJ) through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF). The FBI is designated the lead agency to direct the NCIJTF and any law enforcement activities. Threat response includes countering malicious cyber activity and conducting criminal investigations. Other components of threat response include attribution, pursuit, and disruption of malicious cyber activity and actors [2].

Asset response activities are focused on recovery from the cyber incident and future mitigation efforts. The National Cybersecurity and Communications Integration Center (NCCIC), an entity of DHS, leads asset response activities. The NCCIC is one of two centers operated by DHS's Cybersecurity and Infrastructure Security Agency (CISA). Asset response involves protection activities such as mitigation of vulnerabilities during malicious cyber activity. Restoration of services, lessening impact, and assessing risk to other assets are additional asset response actions taken in reaction to malicious cyber activity [2].

Intelligence support and related activities support both response efforts by providing relevant information. The Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center (CTIIC) leads this line of effort. CTIIC uses a top-down approach to provide intelligence support to federal cyber centers. CTIIC is a multiagency center that integrates intelligence analysis in support of DHS and FBI response actions to a significant cyber incident [2].

A thorough explanation of the required U.S. government's efforts to respond to a cyber incident is presented in the National Cyber Incident Response Plan [3], one of many follow-on efforts in response to the PPDs. The authorities and statutes upon which the plan relies further establish the roles and responsibilities of government entities to not contradict established laws and precedents. For example, the limitation of the Department of Defense's (DOD) role in protection of critical infrastructure and response to cyber incidents reflects the U.S. Code (USC) Title 10 authorities governing the armed services.

DHS's critical infrastructure roles and responsibilities are broad. DHS must protect critical infrastructure and manage cybersecurity risks across all sectors. DHS is also responsible for resource allocation and prioritization of efforts based upon its understanding of risks and consequences of incidents against particular sectors, and DHS is specifically responsible for identifying critical infrastructure at the greatest risk [4]. Per the 2018 DHS Cybersecurity Strategy, "DHS must improve the cybersecurity of critical infrastructure through the development of tools, services, and other offerings, as well as through targeted outreach to critical infrastructure owners and operators, service providers, and other key enablers of risk management activity" [4].

The breadth of roles and responsibilities for the DOD may be narrower than those of DHS, but the DOD is directly involved in the task of strengthening the security and resilience of critical infrastructure. The DOD is responsible for defending its own networks and systems and is potentially responsible for defending sectors of critical infrastructure directly tied to national defense activities. To support defense of critical infrastructure networks, the DOD conducts operations on foreign networks and provides indications and warning to public and private sector partners [5]. The DOD's efforts in foreign networks complements DHS's efforts domestically to enhance coordination of the whole-of-government to defeat malicious cyber activity.

D. THESIS ORGANIZATION

The remainder of this thesis examines what has been defined as critical infrastructure and whether the functions performed by DHS, DOD, and other government entities adequately address the security and resilience of critical infrastructure. A synopsis of critical infrastructure, as defined by each sector-specific agency, with a focus on the relationship to cyberspace provides an understanding of the scope of critical infrastructure. The impact of PPD-41, United States Cyber Incident Coordination, is then examined as it relates to the defense of critical infrastructure from cyber incidents. An assessment of the organization structures of DHS and supporting roles of other federal agencies, including the DOD, is provided as well, and additional federal policies and resources are examined

for refinement of tasks, actions, and authorities of various government entities, as relating to protection of critical infrastructure from cyber threats.

Chapter II provides an examination of U.S. government organization and areas of progress since PPD-21 and PPD-41 were enacted. The structure of DHS has changed and possibly advanced its critical infrastructure protection efforts. Areas of progress or supplemental U.S. government policy addressing critical infrastructure are noted within the chapter. The chapter provides some change in perspective from the large scope, sector-specific framework of critical infrastructure towards a more refined approach.

Chapter III examines the scope and scale of critical infrastructure by sector, with a focus on the cyber components of each sector. Risks and threats to the sector are identified. Additionally, each sector is evaluated on criteria defined in Chapter II.

Chapter IV describes several cyber attacks against critical infrastructure. The attacks, effects of the attacks, and subsequent actions by the U.S. government are examined and summarized. Attacks are framed in the context of critical infrastructure, categorized by the affected sector of critical infrastructure, and analyzed in a manner supporting generalized conclusions.

Chapter V concludes this work with key points and recommendations.

II. ORGANIZATIONAL STRUCTURE AND PLAN DEVELOPMENT

A. REQUIREMENTS AND ACTIONS

As stated in PPD-21, DHS is responsible for providing the strategic guidance that promotes the national unity of effort upon which effective critical infrastructure security relies. The following sections examine specific tasks directed in PPD-21 to DHS, the sector-specific agencies, and other components of government. Following that, the plans developed, partnerships utilized, and the organizational structure of DHS are analyzed in the context of the cyber aspects of critical infrastructure.

The first strategic imperative of PPD-21 is to refine and clarify functional relationships across the federal government in support of the national unity of effort towards security and resilience of critical infrastructure. Stated differently, DHS is responsible for defining critical infrastructure security relationships in line with the roles and responsibilities assigned to organizations.

An additional PPD-21-prescribed DHS responsibility is coordination with sector-specific agencies to identify and prioritize critical infrastructure. Identification and prioritization of infrastructure is partly accomplished through the sector-specific plans. Additional efforts such as hosting sector taxonomies on DHS online portals allow for more thorough identification efforts of assets. DHS accepts sector inputs and then prioritizes infrastructure based on the National Critical Infrastructure Protection Plan (NCIPP). The NCIPP is further examined in Chapter III, Section D.

An explicit DHS responsibility is creation of two operations centers: the National Infrastructure Coordinating Center (NICC) and the NCCIC. These operations centers are respectively responsible for physical infrastructure and cyber infrastructure. The NCCIC includes U.S. Computer Emergency Response Team (US-CERT), as previously noted, and also the Industrial Control System Cyber Emergency Response Team (ICS-CERT).

PPD-21 prescribes additional roles and responsibilities for DHS and the sector-specific agencies, and there are additional federal responsibilities delineated as well. These

responsibilities pertain to coordination efforts, reporting requirements, and support functions. DHS is required to work with sector-specific agencies conducting risk management, to coordinate federal response actions to significant incidents against critical infrastructure, and to broadly support sector-specific agencies in security activities. Implementation of the directive also includes a requirement to update the National Infrastructure Protection Plan (NIPP).

B. THE NIPP, PARTNERSHIPS, AND THE CYBERSECURITY FRAMEWORK

The NIPP applies to owners and operators of critical infrastructure, sector-specific agencies, and any person or entity that has equities in some aspect of critical infrastructure. The goal of the plan is to outline and guide national efforts in strengthening the security and resilience of critical infrastructure. The plan was "developed in a collaborative process with input from all 50 states and stakeholders from all sectors of critical infrastructure [6]." The plan provides goals, priorities, methods for evaluation, and a cycle that allows for continual input by all entities to whom the plan applies.

First published in 2009, the NIPP was updated in 2013 in response to PPD-21's promulgation. The update establishes security and resilience of critical infrastructure as the primary aspect of planning efforts. The NIPP acknowledges the diverse aspects of critical infrastructure and states that the plan itself is meant to be flexible and adaptable to the broad spectrum of critical infrastructure. Public and private sector partnerships are highlighted as a key ingredient to the unified effort necessary to strengthen the security and resilience of critical infrastructure.

The NIPP defines cyber threats as part of the overall risk environment and integrates cyber and physical threats into a single risk management process. The risk management process is a cycle of setting goals, identifying assets, analyzing risks, implementing mitigations, and measuring effectiveness. Information sharing is a required aspect of each step in the cycle. Per the plan, risk management is required by each entity involved in protections of critical infrastructure from the owner and operators to federal government. Partnerships bolster the risk management process by enabling greater

information sharing. As far as prioritization of cybersecurity of critical infrastructure, the NIPP states:

> Critical infrastructure community is doing well with integrating cybersecurity into core business practices, but government is not doing a good job of maintaining funding to infrastructure that requires continued investment, such as water, wastewater, energy, etc. This indicates that government priorities need to be shifted to physical infrastructure, while allowing private sector to continue investing in cybersecurity. [6]

The core tenet of partnerships referenced in the NIPP is collaboration between public and private sectors of critical infrastructure. The Critical Infrastructure Sector Partnerships Advisory Council (CIPAC) was first established by the Secretary of Homeland Security in 2006, with the latest charter signed in 2018. It serves as a mechanism for public and private sector forums. Through the CIPAC model, each critical infrastructure sector independently engages security activities, and the CIPAC facilitates intra-sector and cross-sector engagement. The CIPAC is incorporated into the NIPP and follows implicit and explicit requirements of PPD-21 that pertain to information sharing and partnerships among private sector and government entities that have shared critical infrastructure equities. The CIPAC holds periodic meetings with agendas intended to foster stakeholder discussion. For example, in October 2018 a meeting with the Election Sub-Sector of the Government Facilities Sector was held to discuss working groups and a strategic schedule for security efforts in support of the November elections [7]. The CIPAC is not legally required to publish meeting minutes making it easier to promote more frank discussions between partners.

The CIPAC includes government coordinating councils (GCC) and sector coordinating councils (SCC) for each sector of critical infrastructure and is the partnership construct that facilitates interaction between government and private-sector entities. The CIPAC assists government in policy advisement and critical infrastructure security efforts. The composition of the SCCs requires recognition by the sector-specific agencies [8]. The SCCs are organized and governed by private sector industry partners, such as owners and operators or industry trade groups. The SCCs are the primary points of collaboration between private sector and government. Each SCC approves a charter that establishes

objectives, membership, and other council-specific rules, such as leadership of the council. Council leadership is either elected by council members or comprised of founding members, depending upon the sector. SCC participation is voluntary and is not intended to inhibit sector members from establishing direct relationships with DHS or sector-specific agencies. For example, the SCC can promote National Institute of Standards and Technology (NIST) cybersecurity standards across the sector, then collect feedback and provide to the sector-specific agency for sector-specific cybersecurity standards. This collaborative cycle was used by the Nuclear Reactors, Materials, and Waste Sector for development and implementation of a sector-specific Cybersecurity Framework.

The SCCs are primarily intra-sector entities. The GCCs, on the other hand, work across sectors. The GCCs are chaired by representatives chosen by the respective sector-specific agencies and are comprised of federal, state, and local government entities [9]. The GCCs are therefore in a position to facilitate coordination across jurisdictional boundaries for all levels of government. When called for, GCC membership also includes representation from regulatory agencies. For example, the Federal Communications Commission (FCC) is a member of the Communications and Information Technologies Sectors' GCCs; the Nuclear Regulatory Commission is a member of the Nuclear Reactors, Materials, and Waste Sector GCC.

The charter for each SCC and GCC establishes its meeting requirements, typically quarterly. The GCCs are primarily responsible for drafting and implementing sector-specific plans, but the SCCs are essential to collecting data and inputs from the owners and operators. Both councils are responsible for promoting participation in sector-specific activities to include exercises, information sharing networks, and risk management processes.

Partnership structures are standardized across critical infrastructure sectors, though information sharing methods differ. DHS hosts material for eight critical infrastructure sectors, CISA, and the Department of Energy (DoE) on the Homeland Security Information Network (HSIN), and each sector uses the hosted information for sector-specific reasons. The Dams Sector hosts its taxonomy on a dedicated HSIN portal. Other sectors access threat intelligence via the more general critical infrastructure portal. The Treasury

Department, in its role as sector-specific agency, uses its Cyber Intelligence Group to evaluate and disseminate sector-specific threat information in collaboration with the Financial Services information sharing and analysis center (ISAC) (an organization created by owners and operators of critical infrastructure on a voluntary basis for threat mitigation and related efforts [10]). The Food and Agriculture GCC and SCC each have dedicated HSIN portals, and DHS also releases alerts, warnings, and threat bulletins directly to the sector's GCC and SCC.

As directed by the 2013 NIPP, the Joint National Priorities for Critical Infrastructure Security and Resilience were drafted [11]. These priorities are intended to be used by the sector-specific agencies to facilitate development and maintenance of sector-specific plans. The priorities allow sector-specific agencies to focus their efforts in order to reduce risk to national critical functions, enhance incident response and recovery capabilities, improve information sharing, and protect critical infrastructure against nation-state cyber threats. The priorities are focused on risk management and prioritization of cyber and physical threats.

Developed by the NIST as directed by Executive Order 13636, the Framework for Improving Critical Infrastructure Cybersecurity guides risk management to cyber threats against critical infrastructure [12], [13]. The framework was specifically developed in support of cybersecurity of critical infrastructure, though it is intended to be useful to organizations in any industry. Similar to the NIPP, the framework facilitates standardization of risk management processes for the improvement of critical infrastructure security and resilience.

The NIST Cybersecurity Framework guides an organization through an adaptive process to ensure secure and resilient networks. The process aids an organization in establishing necessary functions its networks provide, identifying assets, assessing threats and vulnerabilities, applying mitigations, and protecting its functions. Once a protected network is established, the process provides approaches to detection, response, and recovery from cyber incidents. One line item of the framework core states that an organization receives threat intelligence from information sharing forums. This particular

excerpt is the only element of the framework that ties directly to the NIPP and sector-specific plans on information sharing.

C. DHS ORGANIZATIONAL STRUCTURE FOR CRITICAL INFRASTRUCTURE

Evolved from the National Protection and Programs Directorate (NPPD) within DHS, CISA was established in 2018. NPPD was responsible for the national security mission of DHS, and that mission is refined and elevated by the CISA Act of 2018. As part of the CISA Act, various organizations within DHS were realigned for efficiency of effort [14]. CISA's primary responsibilities focus on the support of security and resilience of critical infrastructure.

CISA develops and oversees implementation of directives, enforceable under the authority of DHS, that apply to federal entities that operate networks within the ".gov" domain. For example, DHS directed the removal of Kaspersky branded products from federal networks in a 2017 binding directive [15]. CISA ensures compliance with the directive for all networks operating on the federal domain.

The two centers required to be established under DHS by PPD-21, the NICC and the NCCIC, are also components of CISA. Both centers provide 24/7 support, and fulfill similar information sharing requirements. The NICC provides situational awareness of critical infrastructure for the federal government [16]. NCCIC activities include incident response and recovery in particular [17].

US-CERT, a previously independent entity, is integrated into NCCIC and is thus a part of CISA as well. US-CERT publishes alerts and other cyber threat or vulnerability messages, as it did before alignment under CISA. Alerts are publicly available and are often directed at private sector industries.

In addition to the PPD-21 directed sector-based approach to combating the risks to critical infrastructure, DHS utilizes a systematic approach to cybersecurity that centers on National Critical Functions. National Critical Functions are defined as, "The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic

security, national public health or safety, or any combination thereof" [18]. In its overview of National Critical Functions, CISA states, "The National Critical Functions construct provides a risk management approach that focuses on better understanding the functions that an entity enables or to which it contributes, rather than focusing on a static sector-specific or asset world view" [18].

CISA implements the systematic approach of National Critical Functions through the National Risk Management Center (NRMC), another collaborative center that works with private sector, government entities, and other stakeholders [19]. Functions are organized into four categories: connect, distribute, manage, and supply. The NRMC views critical infrastructure holistically, solicits input from each sector, and identifies and defines functions that are essential to secure and resilient critical infrastructure. For example, the Conduct Elections function is categorized in the manage category. The NRMC works with stakeholders across the public and private sectors at federal and local levels to characterize the process of conducting elections. The NRMC then engages with CIPAC and stakeholders within the Elections Infrastructure Sub-Sector of the Government Facilities Sector to identify and prioritize critical infrastructure. Finally, the NRMC provides refined risk management support for stakeholders and oversees the risk management process.

D. CONTINUING EFFORTS

In 2017, the President signed Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [20]. This order rearticulates the importance of cybersecurity and asserts that a cybersecurity risk to any one department of government or sector of critical infrastructure can pose a risk to overall national security. With this in mind, heads of federal agencies and departments are directed to identify and prioritize the greatest risks to their respective organizations. They are also directed to identify ways to assist owners and operators of critical infrastructure in protecting against cyber threats. The order also promotes a working Internet that is protected and allows for the achievement of national objectives in cyberspace.

As part of its cybersecurity efforts, DHS, through CISA, publishes reports called Insights that offer background information on a wide variety of cyber-related topics. For

example, there are Insights on *Ransomware Attacks*, *Enhanced Chemical Security During Heightened Geopolitical Tensions*, and *COVID-19 Disinformation Activity* [21]. Insights are intended to provide information that will aid owners and operators in countering cybersecurity risks to critical infrastructure.

Election security represents a key area of evolution and success, as it relates to the government's efforts to strengthen the security and resilience of critical infrastructure. As noted, election infrastructure is a sub-sector of the Government Facilities Sector of critical infrastructure, and "Conduct Elections" has also been designated a National Critical Function [18]. CISA and its operations centers are engaged and provide continuity of effort and information sharing, and CIPAC efforts to establish priorities among sector partners, as it did during the October 2018 meeting, are ongoing. As a result, when federal and state elections are looked at from infrastructure and function perspectives, the focus and protection mechanisms are already established.

E. SUMMARY

DHS is leading efforts to develop partnerships and share intelligence, and they are utilizing a functions-based approach that effectively augments the PPD-21-directed sector-based approach to critical infrastructure security. The NIST Cybersecurity Framework is currently implemented or in the process of being implemented by all critical infrastructure sectors and has received positive feedback. The implementation of the Cybersecurity Framework and risk management processes indicates that the policies and partnership mechanisms, specifically PPD-21, Executive Order 13636, and CIPAC, facilitates a standardized approach to enhancing critical infrastructure cybersecurity. DHS has implemented an adaptable and capable approach to accomplishing the task of strengthening the security and resilience of critical infrastructure.

III. SECTOR ANALYSIS

According to ADM Rogers (ret.), former Director of the National Security Agency (NSA) and Commander U.S. Cyber Command, "As I think many of you are aware, the U.S. government has designated 16 segments within the private sector as being of critical significance to the nation's security. Think water. Think power. Think aviation, financial - 16. U.S. Cyber Command is tasked to be prepared to provide DOD capability to defend that infrastructure" [22]. ADM Roger's statements during his testimony before the House Intelligence Committee in November 2014 outlined the DOD's involvement in the defense of critical infrastructure. His statements also highlighted the threats to critical infrastructure posed by sophisticated malware possessed by nation-state adversaries.

During ADM Rogers' testimony to Congress four years later, he stated, "We need to reconsider what is Critical Infrastructure in the digital age" [23]. It was asserted in a *Homeland Security Affairs* essay that "Critical Infrastructure isn't critical" [24]. The essay focused on the September 11, 2001, attacks in New York City, but provides a relevant perspective that adds to the assertion that critical infrastructure is poorly defined. From the essay:

> While it was unforeseeable at the time, the Lower Manhattan area that was most heavily impacted by the September 11, 2001 attacks is more valuable today and better positioned for the future than it was prior to 2001. If terrorists cannot cripple this nation by toppling 100-story commercial high-rise buildings, what kinds of facilities would have a debilitating impact on the entire nation if they were destroyed? Instead of being designated "critical," the majority of infrastructure facilities are insignificant to the functions of the overall system because the loss of these facilities does not cause widespread disruptions to the nation, region, or even the local area. The worst circumstances may spur the greatest opportunity for positive change, which could shift homeland security strategies to focus primarily on effective recovery rather than protecting existing systems...A solution for accomplishing the task of effectively identifying, prioritizing, and protecting CI is to refine the criteria for how facilities are determined to be critical. A lower number of critical facilities will reduce the overall scope of the protection mission. Adopting a risk-based approach for both prioritization of facilities and evaluation of national impacts can assist DHS in more effectively designating facilities as "critical." [24]

Notwithstanding that the notion of critical infrastructure may be inadequately defined or that categorization by sector may be deleterious to its security, the relevant critical infrastructure policy and literature do follow sector categorization. The following examination, therefore, takes the same approach. This by-sector examination includes a description of each sector's profile, with specific attention paid to the cyber aspects; risks to the sector; and unique legislation or policy that governs the sector. The risks identified are specific to cyberspace, but not exclusively so. Some sectors have risks or a history of attacks in the physical domain that in some cases were a catalyst for sector-specific legislation. The examination also provides a cursory look at prioritization of critical infrastructure within sectors, across sectors, and in general.

Some sectors are so decentralized that the feasibility of a cyber attack reaching the level of a significant cyber incident is low, according to the Severity Schema [25]. As part of the Severity Schema calculation, which is utilized by NCCIC for standardizing the severity of a cyber attack on a national scale, weights are assigned to each sector that indicate cyber attacks against some sectors are of greater concern due to their cross-sector dependency. DHS resource allocation is prioritized in line with the weights assigned for the Severity Schema calculations. For example, the Energy Sector has the highest weight due to the determination by DHS and other stakeholders that a cyber attack against the Energy Sector would have the highest likelihood of impacting other sectors.

Each sector-specific plan (a formal plan drafted by the sector-specific agency as a required task of PPD-21) asserts the problem of a cyber attack in terms of the worst-case scenario. The use of a worst-case scenario may be two-fold: the self-interest of the sector-specific agency and the directive nature of PPD-21 and the NIPP. PPD-21 does not require that sectors of critical infrastructure be further prioritized, yet that is what the DHS cybersecurity strategy outlines. The approach to prioritization of critical infrastructure is collaborative between DHS, sector-specific agencies, and coordinating councils that represent critical infrastructure owners and stakeholders.

The legislation that is unique to some sectors can also impact the efficiency of response efforts and the efforts of the U.S. government to strengthen the security and resilience of affected critical infrastructure. In some cases, legislation assigns

responsibilities or actions to additional entities in ways that may hamper cyber incident response actions or prolong coordination efforts by convoluting the relationship between owners and operators and the respective sector-specific agencies. In other cases, byproducts of legislation unrelated to PPD-21 can result in improved security practices.

To provide specific examples of prioritization issues and the legislation that impacts critical infrastructure, it is necessary to define and examine each sector. In the following section, each sector is evaluated on the following criteria: expertise or a notable advantage of the sector-specific agency; promotion of cybersecurity measures by the partnership structure; and legislation, policy, or sector-specific characteristics that enhance security and resilience of the sector. To qualify the evaluation, each sector is noted as well organized to implement security measures, adequately organized, or inadequately organized. A sector meeting all three criteria is considered well organized; meeting two criteria is considered adequately organized; and meeting fewer than two criteria is considered inadequately organized.

The three criteria used to evaluate critical infrastructure sectors are derived from PPD-21 and supported by policy. The first is expertise or a notable advantage provided by the sector-specific agency. Per PPD-21, the sector-specific agency leads its respective sector's security and resiliency efforts and is chosen based on expertise or institutional knowledge. Evaluation of the sector-specific agencies supports the sector-specific approach to critical infrastructure security and resiliency by focusing on the leadership elements of each sector.

The second criterion used to analyze the sector-specific approach to critical infrastructure is promotion of cybersecurity measures by the partnership structure that exceeds the minimum standard. The minimum standard is voluntary use of the NIST Cybersecurity Framework. The partnership structure is important for evaluation of critical infrastructure security because most critical infrastructure is owned and operated by the private sector. Effective public-private partnership is therefore critical to ensuring national unity of effort. The NIST Cybersecurity Framework and the partnership structure are based on prescribed policy, as described in Chapter II, Section B.

The third criterion is legislation, policy, and sector-specific characteristics that enhance or inhibit security and resilience of the sector. PPD-21 notes that each critical infrastructure sector is unique in characteristics and risks, and there are often sector-specific legislation and policies that do not directly pertain to the tasks of PPD-21. The legislation and policies can, however, affect security and resiliency efforts. Sector-specific characteristics such as a functions-based approach to defining the sector or oversight by regulatory agencies can also affect the sector's security and resilience. Evaluating the sector-specific legislation, policy, or characteristics supports the sector-based approach by allowing for a non-standard approach to sector security and resilience.

A. SECTORS OF CRITICAL INFRASTRUCTURE

1. Chemical

The Chemical Sector is comprised of facilities numbered on the order of magnitude of hundreds of thousands. These facilities process, store, and handle various chemicals including everything from sulfuric acid to food additives, from fertilizers and pesticides to bleaches and toothpastes. As of July 14, 2015, 3,227 facilities were regulated by Chemical Facilities Anti-Terrorism Standards (CFATS) and numerous additional chemical facilities are subject to further government regulation. For example, as of 2013, 10,500 licensees and permittees were subject to Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) security rules associated with restrictions imposed on explosives [26].

DHS is the sector-specific agency for the sector. Per the NIPP, sector-specific agencies have expertise in their respective sectors. Through CFATS, DHS has been assigned permanent authority for security regulations of chemical facilities since 2007. The involvement of DHS with chemical facilities is a likely reason for the department's selection as sector-specific agency, but there are nuances to the designation. The entity within DHS that is responsible for the Chemical Sector, for instance, is considered a non-regulatory entity [27].

Between 1970 and 2016, 348 incidents of chemical terrorism occurred globally, including 29 incidents in North America. From April 2009 to April 2019, the number of regulated chemical substances under CFATS increased from 33 million to 149 million [28].

It is difficult to qualify or put these numbers into context: is the number of incidents truly high or simply a result of the large number of potential targets? Nevertheless, it is safe to say that the Chemical Sector is successfully targeted with some frequency.

Regarding cyber threats, the potential for manmade deliberate attacks is well understood. The sector-specific plan states, "Disruptions to these systems could result in theft of intellectual property; loss of operations capacity; or a chemical theft, diversion, or release. A small portion of [industrial control systems] are updated through Internet-accessible systems and third-party devices, which exposes Chemical Sector assets to additional threats from remote attacks" [26]. By implication, the plan recognizes that cyber attacks against industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems of sector facilities can result in toxic releases.

Unlike other critical infrastructure sectors, the federal government specifically regulates cybersecurity for the Chemical Sector [29]. The involvement of the U.S. government in the regulation of cybersecurity for the Chemical sector was initiated with Executive Order 13650, Improving Chemical Facility Safety and Security [30], released in 2013. This executive order bound DHS, the Environmental Protection Agency (EPA), and the Secretary of Labor to tackle issues of safety and security of chemical facilities and risk reduction posed by hazardous chemicals to industry employees and communities. The primary focus of the executive order was the prevention of unauthorized weaponization of chemicals. Cybersecurity regulation of the sector is not an explicit requirement of the executive order but is considered an implicit responsibility.

Subsequent to Executive Order 13650, the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 became law. An extension to the CFATS Act was signed in 2019. The act asserts the necessity of standards and assigns responsibilities to various government departments to more fully carry out responsibilities already directed by Executive Order 13650 regarding risks associated with hazardous chemicals [31].

The responsibility to regulate cybersecurity for the sector is assigned by DHS to members of the sector coordinating councils. For example, the American Chemical Council, a member of the Chemical SCC, facilitates implementation of the NIST

Cybersecurity Framework by owners and operators of sector infrastructure [29]. Though the national cybersecurity framework applies to more than just the Chemical Sector, the requirement to regulate cybersecurity arising from CFATS is a separate, authoritative mechanism levied on the sector-specific agency.

Based on the three criteria, the Chemical Sector is well organized to implement security measures. DHS has institutional knowledge of the Chemical Sector based in its role assigned in CFATS. Through the actions of the sector-specific agency, cybersecurity for the Chemical Sector is enhanced. The scale of facilities is large, but the use of the sector coordinating council members to facilitate implementation of the Cybersecurity Framework across the sector is an effective use of the partnership structure. The additional requirement of DHS regulating cybersecurity through CFATS likely enhances security of the sector. The requirements defined in the sector-specific plan, such as site visits and accreditations of Chemical Sector facilities, also includes cybersecurity standards.

2. Commercial Facilities

The Commercial Facilities Sector is broken into eight subsets: entertainment and media, gaming, lodging, outdoor events, public assembly, real estate, retail, and sports leagues. The sector includes everything from the nation's 1,392 casinos and casino resorts to the 1.1 million malls and shopping centers. It also includes amusement parks, hotels, museums, sports stadiums, and television and movie production facilities [32]. The sector-specific plan states, "The sector is characterized not just by the physical facilities, but the congregation of people, susceptible to terrorist attacks" [32].

DHS is assigned as the sector-security agency of the Commercial Facilities Sector. As stated in the sector-specific plan, significant portions of the sector's infrastructure have open public access and use of the facilities contributes to the positive economic impact of the sector. Primary concerns for the sector are terrorist incidents, such as active shooters, and natural disasters. DHS's role as the sector-specific agency is supported by its management of the Federal Emergency Management Agency (FEMA) and its partnerships with law enforcement agencies. Through FEMA and law enforcement agency partnerships, DHS is well situated to mitigate major risks to the sector.

According to the Commercial Facilities sector-specific plan, "The [Commercial Facilities] Sector is one of the few U.S. critical infrastructure sectors in which terrorists have executed multiple high-profile attacks directly affecting the public, both in the physical and cyber domain" [32]. Based on the history of attacks and the evident cyber threat, the sector-specific agency warns,

> Building management systems—from heating, ventilation, and air conditioning (HVAC) systems, to access control—are increasingly computerized, making a growing portion of operations vulnerable to a cyberattack or information technology (IT) outage. Due to the [Commercial Facilities] Sector's dependency on the Internet and IT, the failure or infiltration of cyber systems would create a significant negative economic impact on the sector. [32]

The potential for attacks against a building management system in this sector therefore poses a threat to public health and safety.

The risks and attack vectors to the sector originating from or facilitated by the cyber domain are numerous. "Malicious actors could use social media to disrupt events, facilitate attacks, or organize flash mobs, but the sites may also contain valuable information that could aid security efforts during an event or recovery" [32]. As the former director of the National Counterterrorism Center stated in his testimony before the Senate in 2015:

> Adversaries have successfully executed point-of-sale attacks on large retailers and hotels to gain access to confidential data, which has cost companies and financial institutions hundreds of millions of dollars. Governments have launched targeted cyber espionage or sabotage attacks, and there has been an increase in "hacktivism," or politically motivated cyberattacks. The Federal Bureau of Investigation (FBI) identified North Korea as the source behind recent cyberattacks that published thousands of confidential company documents online, including personal email correspondences and employee data. [33]

The Commercial Facilities Sector's scope is unlikely to be problematic to DHS's sector-specific agency role because the sector-specific plan places the onus is on the owners and operators within the sector. Whereas there are requirements within the Chemical sector-specific plan for accreditations and site visits by DHS, the Commercial Facilities sector-specific plan has no such requirements. The key accomplishments highlighted in the

Commercial Facilities plan include greater information sharing resources and efforts, such as establishment of a Cyber Working Group, led by DHS.

The Commercial Facilities Sector is adequately organized to implement security measures. Management of the security and resilience of the sector, including the physical and cyber domain, is effectively described and managed, and DHS and the component organizations possess sufficient institutional knowledge. The sector is predominately privately owned, though the establishment of the Cyber Working Group provides an adequate public-private partnership structure to promote cybersecurity across the sector. There are no notable characteristics, policy, or legislation specifically associate with the Commercial Facilities Sector, and the sector-specific plan notes that the sector is under minimal regulations. Further, attacks against this sector are unlikely to result in broad effects beyond the targeted entity.

3. Communications

The Communications Sector is broadly characterized as including physical and cyber infrastructure in the categories of broadcast, cable, satellite, wireless, and wired [34]. Within those categories, Executive Order 13618 directs provision of the following services and programs:

> [Executive Order] 13618 highlights the Federal Government's need to communicate at all times and under all circumstances to carry out its most critical and time sensitive functions. The Communications Sector plays an essential role by working closely with DHS's OEC [Office of Emergency Communication] to establish and maintain NS/EP [National Security and Emergency Preparedness] communication services and programs, including the Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP) Program. GETS and WPS provide priority completion of wireline and wireless calls when the PSTN is congested in an emergency, while the TSP program provides for priority restoration and provisioning of telecommunication circuits following a disruption of service. [35]

DHS is assigned as sector-specific agency. Per the sector-specific plan, the Office of Cybersecurity and Communications (CS&C) within DHS manages the responsibilities of the sector-specific agency for the Communications Sector. The CS&C, along with the

Office of Emergency Communication, perform the defining roles and responsibilities of a sector-specific agency as defined in the NIPP. Under this structure, DHS has the resident expertise to perform as the sector-specific agency. Per PPD-21, the FCC is permitted to utilize its expertise and any of its authorities to partner with DHS to increase sector security and resilience.

The nature of the Communications Sector is such that the effects of a cyber attack can directly affect the sector's functioning. For example, a denial of service attack against an Internet service provider that degrades the functionality of the provider's networks or services would qualify as an attack against the Communications Sector according to PPD-21 and as a cyber incident (and possibly a significant cyber incident) according to PPD-41.

Per the sector-specific plan, one of the primary sector-specific agency roles is inter-sector coordination. Other critical infrastructure sectors are regarded as customers of the Communications Sector. In this regard, the sector-specific plan refers to lifeline functions specified in the NIPP: communications, energy, transportation, and water. In other words, the NIPP has included communication as a basic and essential function to the operation of critical infrastructure in general, so attacks against the Communications Sector can affect other sectors as well.

Based upon the definition in PPD-21, critical infrastructure provides an essential service to the nation. In particular, energy and communications systems are classified as uniquely critical because all critical infrastructure sectors rely on the functions those systems provide. The NIPP similarly characterizes communications as a lifeline function and emphasizes that lifeline functions require special attention from sector-specific agencies to prioritize infrastructure and identify cross-sector interdependencies. Towards this end, Executive Order 13618 establishes the criticality of specific communications networks and functions.

Taken together, PPD-21, the NIPP, the sector-specific plan, and the executive order have prioritized based upon lifeline function and infrastructure. Responsibility for strengthening the security and resilience of Communications Sector infrastructure belongs to CS&C. Per the sector-specific plan, the communications services and programs specified

in Executive Order 13618 are a responsibility of a specific DHS office that is well-aligned with the Communications Sector. The sector-specific plan also notes that sectors dependent on communications as a lifeline function are responsible for their own redundant communications, appropriately placing communications resilience of other sectors under their respective sector-specific agencies.

Based on the examination above, the Communications Sector is considered adequately organized to implement security measures. The sector-specific agency has appropriate institutional knowledge. Given the functions-based sector profile and the designation as a lifeline function, the prioritization of sector infrastructure and dedication of a separate DHS office by Executive Order 13618 is a notable benefit. There is, however, no notable promotion of cybersecurity measures by the partnership structure relative to the other critical infrastructure sectors.

4. Critical Manufacturing

The Critical Manufacturing sector is comprised of approximately 250,000 firms that process raw material into specialized parts and equipment that are important to many industries. Sector infrastructure includes the business enterprises that process materials, the raw materials themselves, industrial equipment, and the supporting components that enable the processing from raw materials to final products. Of note, three quarters of these firms have fewer than 20 employees, and fewer than 4,000 firms have more than 500 employees. The Critical Manufacturing Sector also includes production of specialized parts and equipment and facilities that produce components for defense [36].

DHS is the assigned as the sector-specific agency for the sector. According to the sector-specific plan, the Office of Critical Infrastructure Protection (CIP) (now the Infrastructure Security Division) fulfills the roles and responsibilities of sector-specific agency on behalf of DHS. Given the breadth of the sector, it is not surprising that there is no noted expertise resident within DHS that specifically pertains to the Critical Manufacturing Sector.

As a result of disparate specialized production processes, the sector-specific plan states, “A major failure or disruption in the sector could result in significant national

economic impact and lengthy disruptions that cascade across multiple critical infrastructure sectors or regions" [36]. Aside from solely economic impacts, the sector-specific plan identifies at least four specific results of failures or disruptions if the sector is compromised: "A large number of fatalities, significant first year national economic impact, mass evacuations with prolonged absences of six or more months, and a loss of governance or mission execution that disrupts multiple regions or critical infrastructure sectors for more than one week resulting in loss of necessary services to the public" [36]. The sector-specific plan explains the cyber threat to the sector in the following way:

> Manufacturing processes are typically operated by industrial control systems that increasingly use open platforms and common operating systems, rather than proprietary system designs. Cyber intruders may aim to seize control of the systems to disrupt processes, corrupt information sent to facility operators, damage equipment, or steal proprietary information. Intellectual property theft through cyberattacks can threaten competitiveness, affect business reputation, and subject customers to risk from counterfeit products. Intellectual property shared with business partners outside the company also becomes subject to the security risk of partners' systems. [36]

One issue raised in the sector-specific plan is that due to the nature of the sector, many manufacturers may utilize the same software platforms, so an exploit of software used by one manufacturer might have widespread effects across the sector. The WannaCry and Petya ransomware attacks, for instance, impacted owners and operators of this sector's infrastructure long after indications of the attacks were known. In fact, effects to several sector corporations were noted months after the US-CERT published mitigations [37] [38].

The Critical Manufacturing Sector has unknown or undefined intra-sector and inter-sector dependencies, and its infrastructure uses a combination of business networks and ICS and SCADA systems that use common operating systems and open platforms. Many of these unknown dependencies arise from customers in other sectors. For instance, the Defense Industrial Base (DIB) might require a shift in a commercial manufacturing process to produce a specialized defense product, which in turn requires a specialized part to be produced by the Critical Manufacturing Sector. As a result of the unknown interdependencies and common operating systems and open platforms, a cyber attack against a small firm could easily spread to larger firms that have interdependence due to

the nature of manufacturing processes. Alternatively, specialized process of one firm can result in long-term impacts to another critical infrastructure sector.

The sector-specific plan notes that the sector-specific agency is still identifying critical cybersecurity functions and assets. The identification process is the first step in a strategy to unify cybersecurity efforts between the federal government and sector owners and operators. Additionally, the sector promotes use of the NIST Cybersecurity Framework by private sector partners.

Largely as a result of the lack of sector-specific expertise on the part of the sector-specific agency and the poorly understood interdependencies associated with this sector, the organization of the Commercial Facilities Sector is evaluated as inadequate. While the partnership structure adequately promotes cybersecurity measures across the sector, the sector-specific agency does not have the requisite expertise or institutional knowledge to provide sufficient oversight. Further, the unknown interdependencies coupled with increasing use of common software and open platforms across this and other sectors is a notable deficiency.

5. Dams

The Dams Sector of critical infrastructure is tightly defined: "There are more than 90,000 dams in the United States—approximately 65 percent are privately owned and approximately 80 percent are regulated by state dams safety offices" [39]. The Sector includes dams, levees, mine tailings, and navigation locks [40].

DHS is the assigned as the sector-specific agency, however there is no noted sector-specific expertise in DHS. As highlighted in the sector-specific plan, other federal departments and entities of the Dams Government Coordinating Council (GCC) have responsibility for significant portions of the infrastructure. For example, the U.S. Army Corps of Engineers provides oversight to 706 dams, 236 locks, and over 14,500 miles of levees, and the Department of the Interior oversees over 600 dams, reservoirs, and canals. The lack of sector-specific expertise on the part of the sector-specific agency and the disparate organizations responsible for oversight makes partnerships and information sharing extremely important for this sector.

Perhaps due to the specificity of the Dams Sector, the sector-specific plan includes the physical taxonomy of the entire sector. The plan notes the increasing cyber risks posed by legacy systems and increased use of cyber systems for remote operations of ICS and SCADA systems. Remote cyber operation of sector infrastructure has also resulted in centralization of infrastructure controls and operations. This centralization increases the risk and consequences posed by an attack on the cyber elements of the sector. The Cyber Element sections of the sector-specific plan direct stakeholders to comply with the Dams Sector Cybersecurity Guidelines developed by the sector Cybersecurity Working Group for mitigation of the cyber risks [40].

The Dams Sector Cybersecurity Guidelines are a tailored version of the NIST Cybersecurity Framework that was developed by DHS and the GCC for Dam Sector owners and operators. The methodology in both documents is the same. Business owners are intended to use the documents to establish risk-based, repeatable, and adaptable cybersecurity practices through a series of functions that include simple practices, such as using strong passwords, to more advanced management of remote access to cyber systems [41], [12].

The consequences of a successful attack on Dam Sector infrastructure are not oversold. Greater than 10 percent of cropland is irrigated by dams, upwards of 7 percent of U.S. electricity is generated by hydropower plants (with a concentration in the Pacific Northwest, where 60 percent of electricity is generated by hydropower plants), and 43 percent of the U.S. population lives by levees that reduce the risk of flooding [39]. The sector-specific plan states the following:

> Complete or partial dam failure could result in sudden downstream flooding that causes casualties, major destruction and property damage, and catastrophic economic consequences with cascading disruptions to the Electricity, Transportation Systems, and Water Sectors, among others. A levee breach or overtopping could threaten drinking water supplies and reduce pumping system capacity, cause major agriculture damage, and threaten homes and transportation corridors. Navigation lock damage or delay impedes domestic cargo movement of valuable commodities in many sectors. If breached, mine tailings and industrial waste impoundments can harm human health and the environment...Other sectors rely heavily on the support of dams, and an attack on any dam may cause significant harm to

> another sector, with second and third order effects being as catastrophic as a direct attack on any of those supported sectors. [40]

According to the sector-specific plan, most of the sector's infrastructure is regulated at a state level, about four percent is regulated by various federal agencies such as the Tennessee Valley Authority, and some infrastructure is unregulated. While there is no specific policy or legislation akin to CFATS, DHS does host an online portal for the Dams Sector on the HSIN – Critical Infrastructure, where a detailed taxonomy is maintained in order to enhance collaboration between infrastructure owners and operators and DHS [39].

Despite the lack of sector-specific expertise on the part of DHS, the Dams Sector is assessed as adequately organized to implement security measures. Promotion of cybersecurity measures is accomplished through a tailored version of the Cybersecurity Framework and an information sharing platform. A notable benefit to the sector is a relatively tightly defined and regulated sector profile. The tightly defined sector profile provides commonalities of the cyber aspects of sector infrastructure and supports the tailored version of the Cybersecurity Framework.

6. Defense Industrial Base

The DIB Sector is comprised of government and private sector entities on the order of magnitude of hundreds of thousands that support U.S. military defense requirements, either directly or indirectly [42].

The DOD is designated as the sector-specific agency for the sector. Aside from business partnerships and shared expertise, there is an ongoing exchange of sensitive information between the sector-specific agency and the DIB. The trusted relationship between sector owners and operators and the DOD aligns with the DOD's roles and responsibilities as sector-specific agency, as described in the NIPP and sector-specific plan.

The sector taxonomy includes defense systems that if compromised by an adversary could have impacts on national security. As stated in the sector-specific plan, attacks occur with some frequency. Regarding the cyber threat to the DIB, the sector-specific plan notes:

> The most serious threat to the DIB is the cyber threat. The DIB relies on commercial-off-the-shelf (COTS) information system products that are

> often flawed in their design and implementation, thus offering a host of vulnerabilities to those who would exploit them. The vulnerabilities are sometimes significant and other times too subtle to detect easily. In fact, these vulnerabilities are the subject of widespread exploitation efforts by individuals and groups within and outside the U.S. [42]

While the cyber threat is identified as the most serious threat to the sector, a cyber attack to this sector would be unlikely to rise to a significant level, partially due to the low weighted cross-sector dependency score assigned in the Severity Schema [25]. As stated in the sector-specific plan, "Based on longstanding experience, the DIB [sector-specific agency] expects that the potential DIB impact on public health and safety will not rise to the level of national significance. The DIB [sector-specific agency] postulates the potential adverse impact on the national economy from an isolated DIB disruption or failure to be insignificant" [42].

There are unique aspects to the cyber infrastructure within the sector, but no legislation specifically targeted at these sector-specific threats. While voluntary, there is a prescribed method for establishing trusted relationships and inclusion in designated, protected networks (DIBNet) to facilitate sharing of sensitive information between sector partners and DOD. According to the sector-specific plan, "[Defense Contract Management Agency] conducts assessments on risks and vulnerabilities across the sector. Ultimately, it is understood that cyber attacks occur with some regularity against assets within the sector. Impact of the attacks are assessed based on the scope and victim of the attack. The attacks are often in the form of data exfiltration" [42].

The DIB sector-specific plan provides for intra-sector infrastructure prioritization, using a consequence-based approach to determine how the sector's infrastructure, if unavailable, would degrade DOD mission requirements. Based upon quantitative and qualitative assessments, a sector asset may be prioritized by designation as critical infrastructure and key resources (CIKR). Per the DIB sector-specific plan, the DOD collects more detailed information on CIKR assets, and networks of those assets may be subject to DIB cybersecurity activities.

The DOD's approach to sector security differs from DHS's approach for specific reasons. First, the DOD is the sector-specific agency for only one sector, so their efforts

are more focused. Additionally, cyber attacks against the DIB Sector may directly affect the DOD. For example, compromise of proprietary information on the network of a defense contractor could lead to compromise of a weapons system utilized by the DOD. Conversely, compromise of a network within the Commercial Facilities Sector is unlikely to have a direct consequence on DHS. That DOD's own interests are directly furthered by effective sector security further incentivizes their efforts as sector-specific agency. Finally, DOD also builds trusted relationships with sector partners through statutory acquisition and support processes and can therefore subject those partner networks to DOD requirements.

Based on this examination, the DIB Sector is considered well organized to implement security measures. The DOD has trusted relationships and institutional knowledge to support its role as sector-specific agency. There are mechanisms for utilization of a secure network by sector partners that includes additional cybersecurity measures and regulations. Additionally, there are notable security benefits to the method of developing trusted relationships between the DOD and private sector partners and the assessments and risk evaluation performed through the acquisition process.

7. Emergency Services

Law enforcement, public works, fire and rescue services, emergency medical services, and emergency management are the subcomponents of the Emergency Services Sector. Within these subcomponents is a complex array of personnel, services, and systems. There are over 12,000 local police departments and 73 federal law enforcement agencies. There are over one million firefighters. Emergency management includes Hazardous Materials Response Units, bomb disposal teams, and public safety dive teams. There are almost 6,000 public safety answering points for the 9-1-1 system. Finally, there are drainage and flood control systems, utility systems, and public facilities that all fall under Public Works that are part of this sector [43]. Of the Emergency Services Sector, the sector-specific plan notes:

> The [Emergency Services Sector] is the most geographically distributed sector with more than 2.5 million personnel serving every location in all 50 States, five territories, and the District of Columbia. Security and resilience

> planning and decisions take place primarily at the regional and local level. Complex systems and dispersed assets make it difficult to disable the entire system, but also pose challenges to coordination across disciplines, regions, and levels of government. [43]

DHS is designated as the sector-specific agency. The in-house expertise for the sector resides with FEMA, as priorities of the sector are focused on federal coordination of disaster relief and associated use of emergency services. As noted in the sector-specific plan, protection of the broad array of sector resources is managed through federal, state, local, tribal, and territorial governments and trade organization programs. The scope of the sector infrastructure is beyond the capability of DHS to account for; however, DHS directly supports protection efforts through grant programs.

Not surprisingly, the cyber component of the Emergency Services Sector is woven throughout the sector. There is increasing use of cyber systems for communications and coordination efforts by emergency services, and increased demand for real-time data sharing has led to greater reliance on increasingly complex cyber systems. The sector-specific plan states, "Emergency operations communications, database management, biometric activities, telecommunications, and electronic security systems are conducted virtually and are vulnerable to cyber disruptions" [43]. Technology has facilitated improvements to operations but increased the risk associated with vulnerabilities to these systems. Further, delays or disruptions to cyber systems within the Sector can lead to loss of life.

Based upon Emergency Services sector-specific plan, the greatest threats to the sector are posed by the sector's interdependence on other sectors such as the Communications, Energy, and IT Sectors. For example, a nationally significant attack against the sector is unlikely to result from individual attacks on local emergency service units, but rather from an attack against the 9-1-1 network or other emergency services networks that utilize cyber infrastructure.

DHS's role as the Emergency Services sector-specific agency is similar to its role with the Commercial Facilities Sector in that it focuses on enhancing partnerships. Though, there is a distinguishable difference from the Commercial Facilities Sector and its reliance

on private owners and operators of critical infrastructure. One of the primary forums for information sharing and coordination for the Emergency Services Sector is a subset of the GCC that is comprised of state, local, tribal, and territorial government partners.

Based on the criteria of this thesis, organization of the sector is evaluated as inadequate. The sector-specific agency has institutional knowledge and relatively strong relationships with sector partners due to public ownership of significant portions of the infrastructure by federal, state, and local governments. In the sector's efforts to promote cybersecurity, however, it is difficult to effectively assign responsibility. It is specifically noted in the sector-specific plan, for instance, that there are challenges to determining what level of government is responsible for implantation of cybersecurity standards, such as the NIST Cybersecurity Framework. Until these challenges are overcome, the criterion of effective utilization of partnerships for cybersecurity measures is not met. There is also no legislation, policy, or characteristic that enhances security of the sector. Therefore, the third criterion is not met.

8. Energy Sector

As stated in the Energy Sector sector-specific plan, the sector's infrastructure is categorized into three segments: electricity, oil, and natural gas. The electricity segment is comprised of 6,413 power plants [44]. The oil and natural gas segments are defined by the portion of total national energy output produced by each. Combustion of oil produces one percent of the electricity generated nationally; natural gas produces 22 percent [44]. In fact, unlike most of the other sector profiles provided in the sector-specific plans, there are few metrics put forth to fully describe physical characteristics of this infrastructure sector.

The DoE is designated as the sector-specific agency, as it has appropriate expertise related to the sector's infrastructure. The description of the DoE as sector-specific agency in the sector-specific plan differs from that of the DOD and its roles as sector-specific agency for the DIB. The DIB sector-specific plan describes the trusted relationships and dependencies between the DOD and DIB partners. The Energy sector-specific plan describes the DoE as leveraging its position a federal department to coordinate with DHS,

FEMA, EPA, and the Department of Transportation (DoT) for response actions during disruptions of power supply.

While there have been highly publicized events that indicate U.S. adversaries have infiltrated various segments of the U.S. power grid [45], the threat and efforts to combat the threat are different than what has been portrayed in pop culture and the news media. As a result, considerable government resources can be poorly allocated due to unrealistic concerns when those concerns are echoed by elected officials. Nevertheless, the concerns of a cyber attack against the power grid are not unfounded as demonstrated by events elsewhere in the world such as the disruption of segments of the Ukrainian national power grid in 2015 and 2016 [46].

As one article posted by Axios [47], an online news agency, after consulting cybersecurity experts and government spokespersons stated, there are two problems with focusing more attention on the threat than it merits. The first, is unnecessarily frightening the populace. The second is pressuring government officials to respond to unrealistic threats while desensitizing people to the actual problems. The Axios article also describes the resiliency of U.S. power grids and makes the case that the threat of a cyber attack against the U.S. power grid is oversold to the public.

In 2016, the Mission Support Center of the Idaho National Laboratory released a report titled, *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* [48]. Incidents reported by sector highlighted that the number of reported incidents against the Energy Sector were less than half the number of reported incidents against the Critical Manufacturing Sector. This data point is difficult to contextualize. Scanning and probing accounted for 11 percent of the incidents across all critical infrastructure sectors. The intrusions reported across all sectors included 22 on critical systems. However, the types of incidents are not categorized by sector.

Despite the noted resiliency of U.S. power grids by Axios, disruption of energy services can result in second and third order effects to supported sectors and can result in cascading effects well beyond the Energy Sector. Additionally, successful cyber attacks against the Energy Sector are highly likely to result in physical damage. Physical

destruction is a possible outcome, for example, of a cyber attack that disrupts flow of natural gas through pipelines [49]. Because of the potential for physical damage and effects well beyond the sector itself, and it is for this reason that it has the highest rating of all sectors according to the Severity Schema.

Despite this distinction, there is no specific legislation targeted at this sector.

The sector-specific plan includes several efforts to boost sector resiliency. Aside from developing intra-sector partnerships and working with other federal departments, the DoE developed and promotes a tailored version of the NIST Cybersecurity Framework across the sector. DoE has also taken follow-on actions to work across sub-sectors and identify intra-sector vulnerabilities and risks. Additionally, DoE works with DHS during sector-specific exercises, and exercises are promoted across the sector with varying levels of engagement. For example, Cyber Storm is a recurring sector-wide exercise led by DHS in which DoE fully participates. In addition, emergency response plans developed by DoE include organizational level exercises intended to be conducted by sector owners and operators.

The DoE has significant cross-sector responsibilities. Energy, as a lifeline function listed in PPD-21, is depended upon by all other sectors, and that is reflected in the maximum weighted score of cross-sector dependency in the Severity Schema. The cross-sector dependencies have cyber components that range from control and monitoring to billing functions. The DoE responsibility for response actions in the event of emergency loss of power incidents, as noted in the sector-specific plan, primarily involves coordination with other federal entities.

The sector is evaluated as well organized to implement security measures. The sector-specific agency has the requisite expertise and institutional knowledge and leverages it to the benefit of the sector. DoE also effectively utilizes the partnership structure to refine and promote a tailored version of the Cybersecurity Framework. Partnerships are also reinforced through resiliency exercises across the Sector. As a lifeline function, there is significant cross-sector reliance on the Energy Sector infrastructure. Because of this, the sector's resilience sector is verified through frequent inter-sector exercises. Finally, there

is no additional notable policy or legislation that creates conflicts or impacts sector security.

9. Financial Services Sector

The financial sector includes depository institutions, investment firms, insurance companies, and other banking and financial support institutions. The Financial Services sector-specific plan states, "Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities" [50]. The number of institutions included in the Financial Services Sector numbers in the thousands, and the sector relies heavily on technology, automation, and a secure cyber domain.

The Treasury Department is the assigned the role of sector-specific agency for the Financial Services Sector. The sector-specific plan notes that the Treasury Department has institutional knowledge and expertise related to the sector. It is also noted in the plan that the particular Treasury Department office assigned sector-specific agency responsibilities is not a regulatory entity, a distinction also noted in the Chemical Sector plan.

The Financial Services Sector is a frequent target of malicious cyber activity. According to the sector specific plan:

> Most of the sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity especially important to the sector. Malicious cyber actors continue to target the Financial Services Sector. These actors vary considerably in terms of motivation and capability, but all cybersecurity incidents, regardless of the original motive, have the potential to disrupt critical systems, even inadvertently. [50]

The Treasury Department operates a sector-specific Cyber Intelligence Group to comply with PPD-21 and Executive Order 13636 requirements. According to the sector-specific plan, the Cyber Intelligence Group "identifies and analyzes all-source intelligence on cybersecurity threats to the Financial Services Sector; shares timely, actionable information that alerts the sector to threats and enables firms' prevention and mitigation efforts; and solicits feedback and information requirements from the sector" [50]. The

Treasury Department coordinates with the financial institutions, regulators, and appropriate government agencies such as law enforcement to effectively pursue threats identified by the Cyber Intelligence Group.

The sector-specific plan describes the importance of a public policy framework to overall sector security, but it does not provide detail as to whether there is adequate policy to accomplish the task of strengthening the security and resilience of the sector critical infrastructure. For cyber-specific coordination, the plan references the strength of information sharing and coordination efforts between the sector's respective ISAC, NCCIC, and the FBI.

According to criteria, the sector is assessed as adequately organized. The Treasury Department has sufficient institutional knowledge and expertise and the department maintains robust relationships with financial institutions. The sector's Cyber Intelligence Group provides cybersecurity benefits to sector partners. There is uncertainty, however, as to whether or not public policy framework is adequate. There is no notable sector-specific characteristic that benefits sector security.

10. Food and Agriculture Sector

The Food and Agriculture Sector, like the Commercial Facilities Sector, is almost entirely owned and operated by the private sector and is widely geographically dispersed. To provide a general understanding of the order of magnitude of the makeup of the sector:

> The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity...In 2014, there were more than 935,000 restaurants and institutional food service establishments and an estimated 114,000 supermarkets, grocery stores, and other food outlets. In addition, as of February 19, 2014, there were 81,575 Food and Drug Administration (FDA) registered domestic food facilities (warehouses, manufacturers, processors) and 115,753 FDA registered foreign food facilities. The United States Department of Agriculture (USDA) Food Safety and Inspection Service (FSIS) also regulates 6,755 establishments for meat, poultry, processed egg products, imported products, and voluntary inspection services. Additionally, the United States has roughly 2.1 million farms,

> encompassing 915 million acres of land. Collectively, American farms produce $212 billion in crop production. The top five cash-producing industries are cattle, poultry and eggs, corn, soybeans, and milk. [51]

The Department of Agriculture (USDA) and the Department of Health and Human Services (HHS) are co-sector specific agencies for this sector. HHS executes its sector-specific agency role and responsibilities through the Food and Drug Administration (FDA). The USDA, on the other hand, oversees all agriculture related aspects of the sector and shares responsibility for food safety with the FDA. The co-sector-specific agencies share institutional knowledge and expertise for all aspects of the sector.

Despite decentralization of sector infrastructure, technological advances have potentially increased the threat surface for cyber attacks against the sector. As stated in the sector-specific plan, the sector uses ICS and SCADA systems for production and processing at many facilities. The use of these systems allows for increased connectivity and remote access, but results in greater vulnerability to cyber threats. The sector acknowledges its need to better understand the cyber threat [51].

The sector-specific plan identifies the wide use of ICS and SCADA systems throughout the sector as a commonality of the cyber aspects of the sector. The reliance on infrastructure owners and operators to secure this widely dispersed sector is a notable challenge. Similar to the Dams Sector, the Food and Agriculture Sector utilizes an HSIN portal to disseminate information across the sector. A crux to the information sharing and security efforts within the sector is the verification of critical infrastructure information and identifying members for access to the HSIN portal. This responsibility is assigned to the USDA. Relative to the Dams Sector, the Food and Agriculture Sector is of significantly greater scale making this task more daunting.

The Food and Agriculture Sector is geographically dispersed and comprised of owners and operators of different types and sizes, similar to the Commercial Facilities Sector. While restaurants and grocery store type facilities are part of the sector, the sector-specific plan provides more focus on the sector's industrial components that perform farming, processing, and manufacturing processes. In this context, cyber threats to the sector are similar to those of the Critical Manufacturing Sector in that they are focused on

ICS and SCADA systems. Also similar to the Critical Manufacturing Sector, is the concern that an attack against the Food and Agriculture Sector could be rapidly replicated across the sector because of the use of similar systems. This potential for replication of attacks across the sector is the driving force behind the USDA's requirement to verify critical infrastructure and enable information sharing across the HSIN portal.

For cybersecurity efforts across the sector, it is noted in the sector-specific plan that the USDA relies on DHS's CS&C. Since the primary risks to the sector are animal and crop diseases and food safety rather than cyber threats, so it is reasonable that the sector relies on DHS for cybersecurity efforts. The sector-specific plan requires that cybersecurity practices for the USDA and FDA meet standards of federal policy, and that the federal government cyber assets are secure. Promotion of the NIST Cybersecurity Framework is a priority according to the sector-specific plan, though it is described as a future intended action for the sector.

Organization of the sector is considered inadequate based on only one of the three criteria being met. The co-sector-specific agencies have required expertise and institutional knowledge. The USDA and FDA, however, do not adequately utilize the partnership structure to promote cybersecurity among private sector partners that comprise most infrastructure owners and operators. This shortcoming is most notably indicated by the failure to require utilization of the NIST Cybersecurity Framework and a hands-off approach to cybersecurity within the sector overall. Instead, DHS is primarily responsible for engagement with sector partners on cybersecurity matters. There are not additional characteristics of the sector that enhance security.

11. Government Facilities Sector

The Government Facilities Sector now includes the Election Infrastructure Subsector. In fact, it was the threat of tampering with the subsector during the 2016 Presidential Election that sparked a comment from ADM Rogers (ret.) during testimony to Congress where he declared the necessity of a reconsideration of what is critical infrastructure [23]. At the time, the sector-specific plan was drafted, the sector included more than 900,000 constructed assets belonging to the federal government, as well as assets

belonging to 56 States and territories, 3,031 counties, 85,973 local governments, and 566 tribal nations. In addition to the Election Infrastructure, the assets are divided into the Education Facilities and National Monuments and Icons subsectors[52]. The sector-specific plan states, “Collectively this constitutes one of the largest and most complex sectors within the NIPP framework” [52].

The General Services Administration (GSA) and DHS are co-sector-specific agencies for the Government Facilities Sector. GSA is responsible for support functions of federal agencies. DHS executes its sector-specific roles and responsibilities through the Federal Protection Services, a DHS entity responsible for protection, security, and law enforcement functions in federal facilities. Noted in the sector-specific plan, the Department of Education and Department of the Interior are also assigned roles and responsibilities as sector-specific agencies for the Education Facilities and National Monuments and Icons subsectors, respectively.

The sector also includes special-use military installations, national laboratories, or other “structures that may house critical equipment, systems, networks, and functions” [52]. With such a diverse set of facilities, the Government Facilities Sector is at risk to a wide variety of cyber threats. National laboratories conduct research on sensitive military systems and have been targeted in the past by state-sponsored cyber actors similar to those that have attacked the DIB. The Election Critical Infrastructure was targeted in the 2016 and 2018 national elections by a nation-state adversary [53].

As stated in the sector-specific plan, sector infrastructure is categorized and prioritized by use rather than ownership, since ownership is widely spread across the public and private sectors. If the infrastructure is publicly owned, the sector-specific agencies implement cybersecurity practices in accordance with federal policies and authorities. If privately owned, the sector-specific agencies encourage adherence to the NIST Cybersecurity Framework. The sector-specific plan, relative to other sector-specific plans, more thoroughly emphasizes the cyber risks and incorporates the cyber components of infrastructure into the risk management processes. Then the sector-specific plan ties cyber aspects of the processes directly to the NIST Cybersecurity Framework. This method is

distinct from other sector-specific plans that only reference the NIST Cybersecurity Framework without providing specific guidance.

The sector is well organized to implement security measures. The co-sector-specific agencies have institutional knowledge across the sector and authority over federally owned portions of the sector. GSA and DHS promote measures through the partnership structure to privately owned infrastructure. A sector-specific characteristic that benefits security of the sector is the public ownership of a significant portion of infrastructure, however federal policies and authorities allow GSA and DHS to require cybersecurity measures for publicly owned infrastructure.

12. Healthcare and Public Health Sector

The Healthcare and Public Health Sector, like many of the other sectors of critical infrastructure, is more expansive than its name may immediately indicate. The sector-specific plan for the sector states, "The [Healthcare and Public Health] Sector is large, diverse, and open, spanning both the public and private sectors. It includes publicly accessible healthcare facilities, research centers, suppliers, manufacturers, and other physical assets and vast, complex public-private IT systems required for care delivery and to support the rapid, secure transmission and storage of large amounts of [healthcare and public health] data" [54].

The HHS is designated as the sector-specific agency for the sector. HHS has institutional knowledge and expertise resident in the department.

According to the sector-specific plan, average daily ransomware attacks against the Healthcare and Public Health Sector increased from 1,000 to 4,000 in the period from 2015 to early 2016 [54]. The increasing reliance on IT services for storage and transmission of sensitive health information corresponds to increasing cyber threats. Sophisticated cyber actors threaten security by stealing intellectual property, harvesting personal health information, degrading or denying access to data, among other forms of attack. The HHS Secretary responded to the increased cyber threats by creating the Office of the Assistant Secretary for Preparedness and Response (ASPR), to which he delegated leadership responsibility for implantation of PPD-21 and NIPP activities. The ASPR established the

CIP Program Office to manage security and resilience responsibilities and further collaboration among sector partners.

The CIP Program Office relies heavily on partnerships [55]. While the approach is called unique by the sector-specific agency, the underlying method has similarities to many other critical infrastructure sectors. As with many sectors, there are both public and private equities. Partnerships between public and private sector, in the form of various coordinating councils, is a common form of effort among sector-specific agencies. The primary noted difference is the organizational structure of the sector-specific agency for addressing critical infrastructure protection efforts. The development of the CIP Program Office and the proactive leadership approach to the partnership structure is different from other sectors, such as the Energy Sector, that rely on DHS leadership. For example, the ASPR drafted the National Health Security and Strategy Implementation Plan. that is tailored to the Healthcare and Public Health Sector. Further, the plan the CIP Program Office's leadership in partnership engagement to enhance sector security.

According to HHS, the HHS Chief Information Officer did review and provide inputs to the 2020 budget in order to ensure compliance with the Federal Information Technology Acquisition Reform Act and that efforts are made to secure the cyber components of the sector [56]. However, the HHS budget does not impact private sector healthcare, and there is uncertainty as to where government responsibility starts and ends in protecting the cyber domain of the Health and Public Healthcare Sector. This uncertainty is a deficiency in the security of the sector.

Sector organization is considered adequate based on the criteria. The sector-specific agency has expertise and institutional knowledge, and HHS promotes cybersecurity measures across the sector through its implementation of a dedicated program office. There is no sector-specific characteristic that benefits sector security. Further, unlike Government Facilities Sector, the Health and Public Healthcare Sector is not in a position to leverage publicly owned infrastructure to enhance sector cybersecurity.

13. Information Technology Sector

The IT Sector may be the most difficult sector of critical infrastructure to identify and enumerate. According to the sector-specific plan, “Unlike many critical infrastructure sectors composed of finite and easily identifiable physical assets, the IT Sector is a functions-based sector that comprises not only physical assets but also virtual systems and networks that enable key capabilities and services in both the public and private sectors” [57]. A successful attack against a critical function of the IT Sector would be significant due to its cross-sector dependency. Of note, the sector’s weighted cross-sector dependency score is second to Energy on the Severity Schema. However, the only cyber attack identified as having a likelihood greater than low is the breakdown of a single interoperable Internet, and this corresponds to the critical IT function of providing domain name resolution services that is specified in the sector-specific plan [57]. Loss of domain name resolution services causes significant degradation to Internet services for potentially significant portions of an Internet.

DHS is designated as the sector-specific agency for the IT Sector. The CS&C carries out the role and responsibilities of sector-specific agency on behalf of DHS. There is no specific expertise noted in the sector-specific plan. As a result, IT Sector security substantially relies on the Sector Coordinating Council which includes Internet service providers, DNS (domain name system) root and Generic Top-Level Domain operators, communications companies, software companies, and others [57]. When gauging what government’s role should be in protecting the sector from cyber attacks, it worth noting that the sector is comprised of those entities that keep the Internet functioning on a daily basis and that those entities may be better positioned than government agencies to protect sector assets.

The role DHS takes as sector-specific agency for the IT Sector is noticeably different than for other sectors to which it is assigned as sector-specific agency. DHS leads partnership engagements and activities, like it does for other sectors, though the culmination of its engagement activities in this case is a series of cybersecurity exercises. According to the sector-specific plan, the cybersecurity exercises of the IT Sector are the most comprehensive government-sponsored exercises of their kind. Instead of validating

sector infrastructure, such as the sector-specific agency does for the Dams or Food and Agriculture Sectors, DHS works with sector councils to delineate sector critical functions in a rapidly changing technology-driven landscape. The distinctly different approach to a functions-based sector when compared to the approach to a facilities-based sector demonstrates an adaptability of DHS in its role as sector-specific agency.

Based on the above analysis, sector organization to implement security measures is evaluated as adequate. The sector-specific agency does not have significant sector-specific institutional knowledge or any noted advantage, but it does have a robust Sector Coordinating Council upon which it can rely. DHS effectively promotes cybersecurity measures through partnerships and collaboration to define critical functions and prioritize security efforts across the sector around those functions. Additionally, the sector-specific plan notes that DHS is engaged with partners to develop a tailored version of the NIST Cybersecurity Framework. A sector-specific characteristic that enhances security is the frequent conduct of cybersecurity exercises focused on the security and resilience of the sector's functions-based infrastructure.

14. Nuclear Reactors, Materials, and Waste Sector

At the opposite end of the spectrum from the IT Sector, with regards to scope, is the Nuclear Reactors, Materials, and Waste Sector: "The Nuclear Sector is the most closely regulated of all infrastructure sectors, and the nuclear industry has taken additional steps to protect assets, respond to and recover from incidents, and enhance resilience" [58]. The sector is also limited in scale, relative to the other Sectors, with the following components [59]:

- 99 Active Power Reactors
- 18 Decommissioning Power Reactors
- 31 Research and Test Reactors
- 8 Active Nuclear Fuel Cycle Facilities
- 20,000 Licensed Users of Radioactive Sources
- Over 3 Million Yearly Shipments of Radioactive Materials

DHS is designated as the sector-specific agency for the sector, and the Infrastructure Security Division executes these responsibilities. Per the sector-specific

plan, the Nuclear Regulatory Commission (NRC), an independent federal agency, provides data on sector infrastructure. PPD-21 directs the NRC fulfill its regulatory role and collaborate with DHS in support of sector security and resiliency.

The coordinating councils and the sector-specific agency for the sector have developed a tailored version of the NIST Cybersecurity Framework Implementation Guidance. The sector-specific agency and the coordinating councils recognize the uniqueness of the sector, based upon historical safety trends and a public fear of disaster posed by nuclear power plants [60].

Based on this examination, the sector is well organized to implement security measures. Though, DHS does not have institutional knowledge or expertise, close collaboration with the NRC reasonably mitigates the deficiency. NRC has expertise derived from its regulatory function. DHS promotes cybersecurity via a tailored version of the NIST Cybersecurity Framework. Sector security also benefits from a tightly defined sector profile, similar to the Dams Sector. Finally, the sector benefits from well-regulated infrastructure. As noted in the sector-specific plan, the NRC enforces cybersecurity regulations at each facility, and DHS, as the sector-specific agency, conducts independent review of cybersecurity risks to the sector.

15. Transportation Systems Sector

The Transportation Systems Sector includes numerous public entities and private companies as well as the transportation veins such as roadways, waterways, and railroads. Fortunately, the sector's infrastructure is well categorized and defined. The following is the seven subsectors of the Transportation Systems Sector [61]:

- Aviation includes aircraft, air traffic control systems, and about 19,700 airports, heliports, and landing strips.
- Highway and Motor Carrier encompasses more than 4 million miles of roadway, more than 600,000 bridges, and more than 350 tunnels.
- Maritime Transportation System consists of about 95,000 miles of coastline, 361 ports, more than 25,000 miles of waterways, and intermodal landside connections.
- Mass Transit and Passenger Rail includes terminals, operational systems, and supporting infrastructure for passenger. Public

transportation and passenger rail operations provided an estimated 10.8 billion passenger trips in 2014.

- Pipeline Systems consist of more than 2.5 million miles of pipelines spanning the country and carrying nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. Above-ground assets, such as compressor stations and pumping stations, are also included.
- Freight Rail consists of seven major carriers, hundreds of smaller railroads, over 138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives. An estimated 12,000 trains operate daily. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.
- Postal and Shipping moves about 720 million letters and packages each day and includes large integrated carriers, regional and local courier services, mail services, mail management firms, and chartered and delivery services.

The DHS and the DoT have been designated as co-sector-specific agencies for the sector. The Transportation Security Administration (TSA) and U.S. Coast Guard are executive agents for DHS and execute the roles and responsibilities of co-sector-specific agencies along with the DoT. The TSA and Coast Guard have security responsibilities for aspects of the sector independent of their roles and responsibilities to the co-sector-specific agencies.

The cyber domain of the sector includes "positioning, navigation, tracking, shipment routing, industrial system controls, access controls, signaling, communications, and data and business management" [61]. The cyber domain of the sector spans each subsector. For example, the Highway and Motor Carrier subsector cyber infrastructure includes traffic management systems and cyber systems for operational management. Like many of the other critical infrastructure sectors, the Transportation Systems Sector spans the entire nation.

While the sector-specific plan does not further prioritize subsectors, a DHS press release from late 2018 indicates that further prioritization within the sector was needed [62]. According to the press release, DHS and the Oil and Natural Gas Sector Coordinating Council engaged in a meeting that was led by the TSA Administrator and the NPPD Under

Secretary for the purpose of discussing the Pipeline Cybersecurity Initiative [63]. Other parties involved included the TSA, NRMC, and DoE.

Within two months of the press release, a Government Accountability Office (GAO) report identified significant vulnerabilities and threats to the pipeline systems [63]. The GAO report criticized TSA's implementation of the NIST's Framework for Improving Critical Infrastructure Cybersecurity and TSA's assessments for physical and cyber security. In tandem with the GAO report, the Senate Energy and Natural Resources Committee sent a letter to DHS [48], requesting DHS perform an assessment of pipeline security and associated infrastructure as a response action to the GAO findings. In the letter from the senate committee, TSA is criticized for its shortcomings in protecting the pipelines.

Poor security implementation by TSA and misalignment of sector-specific agency responsibilities for the pipeline subsector negatively impact Transportation Sector security. As noted in the GAO report, TSA is primarily responsible for security of pipeline infrastructure, though the transport of oil and natural gas is described as part of the Energy Sector. Thus, implementation of the Pipeline Cybersecurity Initiative is the responsibility of DHS. The DoT, a co-sector-specific agency has no equities in the pipeline subsector.

In the other two sectors that have co-sector-specific agencies, Food and Agriculture and Government Facilities, the co-sector-specific agencies have aligned responsibilities. For the Food and Agriculture Sector, the USDA is responsible for all aspects of agriculture and the FDA is responsible for food safety. The responsibilities complement each other and the diverse aspects of the sector that encompasses crops, farm animals, processing of foods, restaurants, and grocery stores. For the Government Facilities Sector, one co-sector-specific agency is responsible for the support functions of sector facilities; the other is responsible for the protection of the facilities. Unfortunately, this is not the case for the Transportation Sector, as there are incongruent security responsibilities evident between the DHS and DoE. The DoE has sector-specific agency responsibilities for the transport of natural gas and oil. DHS's TSA has sector-specific agency responsibilities for the pipelines that transport natural gas and oil. Though, the Pipeline Cybersecurity Initiative is led by DHS's NRMC.

As the blistering assessment of pipeline security clearly indicates, organization of the sector is inadequate. TSA and the U.S. Coast Guard, as executive agents of DHS, have institutional knowledge derived from their independent security responsibilities for the sector; however, implementation of the NIST Cybersecurity Framework by TSA is deficient, as noted in the GAO report. There are no sector-specific characteristics that benefit sector security. Also, the competing federal department responsibilities that results from such diverse subsectors is a likely impediment to sector security.

16. Water and Wastewater Systems Sector

The Water and Wastewater Systems Sector is comprised of two components: utilities providing drinking water and utilities providing wastewater services. The drinking water utilities also provide water for services that include fire protection, healthcare, and heating and cooling. Wastewater utilities, on the other hand, treat domestic sewage and wastewater produced from industrial processes. The sector includes both public and private utility services[64].

The drinking water component of the Water and Wastewater Systems Sector is comprised of approximately 153,000 Public Water Systems. Public Water Systems are comprised of three elements, with each element subdivided. The physical element is subdivided into the infrastructure and processes that take water from its origin source and deliver it to the customer. The human element includes employees and contractors that manage and operate all aspects of the sector [64].

The final element of the sector's drinking water component is the cyber element which is divided into three subcomponents. The first subcomponent is the SCADA systems that "are part of integrated control systems essential to operation of drinking water utilities" [64]. The second subcomponent is process systems and operational controls not controlled by SCADA systems. The third subcomponent is the enterprise systems including the business networks that provide customer billing, emails, and other applications.

The wastewater component of the sector includes 16,500 publicly owned treatment works, with services provided to more than 227 million people. The wastewater component

is also divided into the physical, human, and cyber elements that are nearly the same for the wastewater component as they are for the drinking water component of the Sector [64].

The EPA is designated as the sector-specific agency. The EPA is a federal regulatory agency, however the sector-specific plan does not describe the EPA's roles and responsibilities as sector-specific agency.

Sector risks are prioritized according to three categories. The most significant risks are defined as, "Risks that need the Water and Wastewater Sector's most urgent attention and greatest resources, based on the pervasiveness of the threat or the potential high impact. Priority activities should directly mitigate one or more of these risks" [64]. The sector's Strategic Priorities Working Group prioritized "cyber events" within this most significant risk category.

The EPA and other members of the sector were recently involved in research at the Department of Energy Idaho National Laboratory to investigate potential effects of a cyber attack on a water utility. Based upon the research, the EPA promulgated the following to sector partners [65]:

> Cyber-attacks on water or wastewater utility business enterprise or process control systems can cause significant harm, such as:
>
> · Upset treatment and conveyance processes by opening and closing valves, overriding alarms or disabling pumps or other equipment
> · Deface the utility's website or compromise the email system
> · Steal customers' personal data or credit card information from the utility's billing system
> · Install malicious programs like ransomware, which can disable business enterprise or process control operations
>
> These attacks can: compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence, and result in financial and legal liabilities. [66]

Compared to sectors with regulatory bodies sector cybersecurity is insufficiently addressed. For example, cybersecurity of the Chemical Sector and the Nuclear Reactors, Materials, and Waste Sector is regulated by DHS and the NRC as part of the regulatory responsibilities of each entity. The Water and Wastewater sector-specific plan defines the

cyber elements of the sector's infrastructure, and the EPA conducts research into cyber threats and publishes information on the potential effects of a cyber attack against the sector. There is no effort, however, at implementation oversight or cybersecurity accountability noted in the sector-specific plan.

Based on these observations, sector organization to implement security measures is assessed as inadequate. The sector-specific agency has the requisite institutional knowledge and authority derived from its regulatory role. Unfortunately, the sector-specific agency does not promote cybersecurity measures through its partnership structure. There is no notable characteristic of the sector that enhances security.

B. SECTOR-SPECIFIC AGENCY COMPARISONS

Based on the analysis of the previous section, five critical infrastructure sectors can be considered well organized to implement security measures based on the three criteria: Chemical, DIB, Energy, Government Facilities, and Nuclear Reactors, Materials, and Waste. Six sectors were characterized as adequately organized: Commercial Facilities, Communications, Dams, Financial Services, Health and Public Healthcare, and Information Technology. Finally, five sectors were evaluated as inadequately organized: Critical Manufacturing, Emergency Services, Food and Agriculture, Transportation, and Water and Wastewater Systems. Water and Wastewater Systems is the only sector that failed to meet at least one criterion.

DHS is the sector-specific agency or co-sector-specific agency for 10 of the 16 sectors, but its role differs from sector to sector. For example, DHS's primary role with the Commercial Facilities and Emergency Services sectors is management of the partnership structures that facilitate coordination within the sector, across sectors, and with other federal agencies. DHS role with regards to the Chemical Sector, on the other hand, includes the regulation of cybersecurity. In this case, the more authoritative role emerged as a secondary effect of CFATS legislation. For the Dams Sector, DHS facilitates intra-sector oversight of infrastructure taxonomy through a DHS-hosted portal.

The Dams, Energy, and the Nuclear Reactors, Materials, and Waste Sectors have implemented tailored versions of the NIST Cybersecurity Framework that were developed

in part by the sector-specific agencies. Along the same lines, the IT Sector was in the process of developing a tailored version of the Cybersecurity Framework at the time of the sector-specific plan publication. Other sectors implement the NIST Cybersecurity Framework without modification to meet NIPP requirements. In the case of sectors falling under HHS and GSA implementation is hindered by the mix of public and private ownership of sector infrastructure.

For the IT Sector, DHS applies a different methodology for defining infrastructure than it does in its role as sector-specific agency for other sectors in that they manage this sector by its functions rather than its facilities. The use of critical functions is apt for a technology and services-based sector. The critical functions that comprise the IT Sector, though, should not be confused with the lifeline functions characterized in PPD-21 and the NIPP or the National Critical Functions (further defined in section C).

Likely due to the distinctly different subsectors, the DoT and DHS, co-sector-specific agencies for the Transportation Sector, rely on other departments to coordinate sector security efforts more than other sector-specific agencies. The security challenges of the sector are not, however, distinctly different than that of other sectors. The Transportation Sector, like several other sectors, relies on ICS and SCADA systems, and similar to the Dams Sector is evolving towards more remote operations of mechanical functions for its infrastructure.

The Chemical; the Nuclear Reactors, Materials, and Waste Sector; and Water and Wastewater Treatment Sector have regulatory agencies to which they are responsible for administration of their infrastructure. Of these, the Water and Wastewater Treatment Sector is the only sector to have its regulatory agency dual-hatted as the sector-specific agency under PPD-21. Notably, the Water and Wastewater Treatment Sector is also the only one of the three sectors to not have cybersecurity regulated by either its regulatory agency or the sector-specific agency. The dual-hatted function is not necessarily causation for the lapse, however. The sector-specific agency for the Water and Wastewater Treatment Sector has established goals to enhance security of the cyber elements of its infrastructure.

The sector-specific agencies and the corresponding plans align with the NIPP requirements to develop a sector profile, assess risks, and outline efforts to protect critical infrastructure. Sector-specific agencies are responsible for prioritizing within sectors. Section C of this chapter details DHS's responsibility for prioritization across sectors, which is part of the security challenge for critical infrastructure.

C. SECTOR-SPECIFIC LEGISLATION AND DIRECTIVES

There are sector-specific legislation and directives that pertain to certain critical infrastructure sectors. A closer look indicates that this does not implicitly introduce counterproductive ambiguity, conflicts, or redundancy counterproductivity, though. In fact, in some instances, the unique legislation may be aiding prioritization efforts.

The Chemical Sector is directly affected by Executive Order 13650 and CFATS. As previously mentioned, the Executive Order and the standards set forth in CFATS resulted in the Chemical Sector being the only sector with its cybersecurity directly regulated by the federal government. Executive Order 13650 establishes a federal agency working group, and a division of CISA provides one of the three co-chairs.

Executive Order 13618 prioritizes segments of the Communications Sector infrastructure. The order addresses the need for unabated communication between certain components of government related to national security and emergency preparedness. DOD and DHS assigned oversight of the development of systems of communication and long-term strategies. The DOD is assigned responsibility for the needs of the Executive Branch of government with respect to national security and emergency preparedness communications networks. The DHS, on the other hand, is assigned responsibility for sustainment of the same communications networks to ensure continuity of government. Additional responsibilities are assigned to other federal departments. For example, the Administrator of Government Services is directed to maintain a common method of acquisition of equipment by federal entities. None of these conflict with roles and responsibilities delineated in PPD-21; however, so the executive order's impact on the sector's cybersecurity is negligible.

The 2018 Pipeline Cybersecurity Initiative was promulgated by DHS in response to criticism levied against the TSA for lack of pipeline infrastructure security. According to the GAO report, TSA did not provide a standard of implementation for the NIST Cybersecurity Framework [49]. The Pipeline Cybersecurity Initiative is managed by CISA through the NRMC. The initiative prioritizes certain infrastructure within a diverse sector of critical infrastructure and focuses efforts of various partnerships. The GCC for the sector provides a forum for DoT, DHS, and DoE to resolve redundant efforts and in that regard improves the sector's unity of effort.

Existing sector-specific legislation and executive orders do not conflict with the sector-specific agency efforts to strengthen the security and resilience of critical infrastructure. The results of the unique efforts are prioritization of infrastructure within a sector, more refined information flow, and focused efforts within the sector-specific agency. There are no noted instances of legislation- or policy-manded efforts that contradict with PPD-21 or PPD-41 requirements or responsibilities.

D. DHS CRITICAL INFRASTRUCTURE PRIORITIZATION RESPONSIBILITIES AND INCLUSION OF NATIONAL CRITICAL FUNCTIONS

In accordance with the 9/11 Commission Act of 2007, DHS is the lead coordinator in the national effort to identify and prioritize the nation's critical infrastructure. DHS executes this responsibility through the NCIPP, which includes data calls to identify domestic infrastructure that would, if disrupted, cause national or regional catastrophic effects [67]. DHS maintains four levels of critical infrastructure for this purpose based on the following criteria [67]:

> Level 1 (All Sectors): Infrastructure that, if disrupted, could result in very significant consequences to human life, the economy, national security, or property.
>
> Level 2 (Agriculture and Food Sector-Specific): Infrastructure that, if disrupted, could result in significant consequences to international, national, or regional economic stability, national security, or property.

> Level 3 (All Sectors): Infrastructure that does not meet Level 1 or Level 2 criteria but is recognized by Sector leadership to be so important to the Nation as to warrant special consideration.
>
> Level 4 (All Sectors): Infrastructure submitted by each state or territory utilizing their own criteria.

In 2013, the GAO released a report critical of the changes DHS made to the criteria for assets added to the NCIPP [67]. According to the GAO, DHS switched to a consequence-based approach for identifying infrastructure that should be on the NCIPP asset list. The GAO declared the approach to be counter to the NIPP and applicable laws. GAO did acknowledged that DHS worked with the sector-specific agencies and other appropriate entities in a proactive manner to assist in nominating assets. Of note, the GAO findings established that DHS's approach may convolute its efforts to apply a common approach across all sectors of critical infrastructure. The GAO recommended, in its 2013 report to Congress, that a peer review of the NCIPP should be conducted.

Possibly the most adverse takeaway from the GAO report is that state-level critical infrastructure partners did not want to participate in the nomination process for adding assets to the NCIPP, citing the cumbersome process and difficulty working with DHS. As noted in the NIPP and sector-specific plans, partnerships are paramount to the security of critical infrastructure. Aspects of the partnerships are voluntary, and private sector critical infrastructure owners and operators are not compelled to take actions directed by the sector-specific agencies, such as implementing the Cybersecurity Framework. Any breakdown in the partnerships adversely affects the security and resilience of critical infrastructure.

Prioritization efforts are a key aspect of DHS's responsibility to strengthen the security and resilience of critical infrastructure. The GAO report acknowledges that critical infrastructure is dynamic, and this is evident in the sector specific plans. The dynamics that must be addressed include evolving technology of the IT Sector and voluntary reporting by infrastructure owners and operators. As noted in the Dams, for instance, sector specific plan, the sector's infrastructure is quantifiable, but ownership has not been identified for all sector infrastructure. DHS is executing its responsibility to prioritize critical infrastructure across all sectors, and the criticisms noted in the GAO report validate the

security challenge presented by the categorization of critical infrastructure. Specifically, the sector categorization of critical infrastructure does not provide for a standard approach by sector-specific agencies to strengthen the security and resilience of critical infrastructure meaning that each agency is free to address the issue as it sees fit.

The CISA is constituted within DHS to execute its national cybersecurity responsibility. CISA "is the Nation's risk advisor, working with partners to defend against todays' threats and collaborating to build more secure and resilient infrastructure for the future" [68]. CISA partners with public and private entities to focus on the threats posed to critical infrastructure, whether those threats are physical attacks by a terrorist, a natural disaster, or cyber attacks from a nation-state adversary. Aside from partnerships across the federal government and private sector, CISA is charged with protecting the ".gov" domain [68]. CISA sits within the hierarchy of DHS alongside the U.S. Coast Guard, the Secret Service, TSA, FEMA, and several other entities [69].

Within CISA exists the NRMC. CISA, as the parent organization, defines NRMC thus:

> NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: Identify; Analyze; Prioritize; and Manage the most strategic risks to our National Critical Functions—the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination. [68]

While National Critical Functions are a focus of the NRMC, CISA addresses critical infrastructure cybersecurity through the PPD-21 sector-based approach. PPD-21 specifically identifies each sector and assigns a sector-specific agency. As noted in Chapter I, the DHS Cybersecurity Strategy defines the cybersecurity role of DHS as including the assurance "that growing cybersecurity risks across all critical infrastructure sectors and other systems that impact national security, public health and safety, and economic security are managed at an acceptable level" [4].

NRMC prioritizes critical infrastructure using a functions-based approach that overlaps with the PPD-21 sector-based approach. For example, the National Critical

Function “Conduct Elections” has corresponding Election Infrastructure that is a subsector of the Government Facilities Sector. Similarly, the National Critical Function “Manage Wastewater” encompasses Water and Wastewater Systems critical infrastructure. The functions-based approach of the NRMC is an additional method of enhancing critical infrastructure security and is further described in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CYBER ATTACKS AGAINST CRITICAL INFRASTRUCTURE

As noted in the sector-specific plans, cyber attacks against critical infrastructure have occurred and are expected to increase in both frequency and sophistication. The following examples provide insight into the breadth of the threat and demonstrate the notion that cyber attacks against critical infrastructure are not isolated events against individual targets but are often complex campaigns lasting years. These examples also provide a lens through which to examine the effectiveness of the PPD-21 development and implementation.

A. NORTH KOREA CYBER ATTACK AGAINST SONY ENTERTAINMENT PICTURES

According to a U.S. investigation, in November 2014 likely North Korean state-sponsored cyber actors infiltrated Sony Entertainment Pictures networks in preemptive retaliation for the planned release of a film that mocked North Korea and its president. The cyber actors exfiltrated and deleted data from company servers and damaged thousands of computers. Most importantly, some of the exfiltrated data was released by the attackers to the embarrassment of the company, and more releases were threatened [70], [71].

Sony eventually declared that the financial effect of the cyber attack was not significant and estimated damage of approximately $15 million (mostly recovered through insurance). Another effect attributed to the cyber attack was the resignation of the Sony Pictures chairwoman due to content of released personal emails that was deemed offensive after public scrutiny. The attack, aside from resulting in the release of damaging information, did prevent the movie from being screened by national movie theater chains. Further, follow-on intimidation in the form of threats to release additional information led some employees to file lawsuits against Sony for not protecting personnel data [71].

In response to the cyber attack, the U.S. government levied additional sanctions against North Korea, published information about the attack, indicted a North Korean cyber actor, and publicly upbraided the North Korean government for its role. The published information included alerts from US-CERT that detailed the cyber actors and methods and

recommended mitigations in the event of future malicious activity. NCCIC declared that DHS and the FBI knew of the cyber actors and their activities since 2009, but no public action had been taken until the effects of the Sony cyber attack [37].

The Commercial Facilities sector-specific plan references the cyber attack against Sony as evidence of increased cyber risks to the sector. Following a series of cyber attacks by North Korean malicious cyber actors, US-CERT published guidance on the threats, malware analysis, and mitigations [72]. The US-CERT guidance is a holistic report on the cyber threat posed by North Korea and concludes that North Korea is capable of cyber attacks against critical infrastructure.

US-CERT-provided guidance also details communication flow between private entities and the federal government for response actions and cybersecurity efforts. Private sector entities are encouraged to contact the FBI when indicators associated with North Korean cyber actors are discovered, and the FBI has mechanisms for directly contacting private sector partners following indications of a potential cyber threat. Per the sector-specific plan, those private sector partners that have established relationships with the FBI and DHS are able to receive more direct intelligence on the cyber threats. For example, the plan details points of contact and partnership structure for accessing the communications channels referenced in the US-CERT guidance. Additionally, U.S. Cyber Command may share foreign threat information with the FBI to aid in investigations of cyber attacks against private sector entities. Information from U.S. Cyber Command and the private sector flows into the same FBI operations center to facilitate efficiency of information sharing and response actions.

Per the NIPP, risk management enhances security and resilience. Though prevention is an important component of security as defined in the NIPP, it is only one aspect of a much broader effort. In this instance, other risk management elements proved more important than prevention, and these proved effective in response to the North Korean cyber attack. Collaborative effort and coordination were touted as key to the success of federal efforts to identify, characterize, and mitigate North Korean cyber attacks. The FBI press release states that Sony notified authorities of the attack within hours and continued to be a valuable partner over the course of the incident response and the investigation that

followed. US-CERT notes the collaboration of the Department of State, DHS, and the Treasury Department in issuing the advisory to alert public and private sectors of the threats posed by North Korean cyber actors. Further, the malware analysis and technical advisories were conducted by CISA, FBI, the Treasury, and U.S. Cyber Command, demonstrating effective unity of effort as required by PPD-21.

The PPD-21 directed tasks were well executed in response to this incident. For instance, the DHS management of response actions and DOD information sharing with DHS cyber centers were effective and well orchestrated. Resilience of critical infrastructure was likely strengthened by Sony's partnership with the FBI during the incident, providing a positive example of private sector entities voluntarily engaging with the public sector to manage incidents, a key aspect of PPD-21, the NIPP, and sector-specific plans. The partnerships described in the sector-specific plans were utilized in response actions. Information sharing of specific threats and mitigations continued from the date of the attacks to present. Finally, these events clearly indicate the importance of the private sector in securing critical infrastructure. In particular, increased security in response to threats is dependent upon information sharing among government entities and private sector partners.

B. RUSSIAN INTRUSION INTO U.S. POWER COMPANIES

On March 15, 2018, an alert was released through US-CERT on "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors" [45]. Within the alert it is stated,

> DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS). [45]

The activity by Russian government cyber actors listed above had been ongoing since at least March 2016. The beginning time frame of the activity is significant, because cyber attacks against the Ukraine power grid disrupted electrical power for limited periods

of time in December 2015 and December 2016 [46]. The attacks against the Ukraine power grid, publicly attributed to Russian state-sponsored cyber actors, indicated that the same cyber actors conducting activity against the U.S. power grid had the capability to launch a similar attack against the U.S. Despite the observed capability, there is no evidence of Russian intent to disrupt power supply in the U.S. A press release by the American Public Power Association, a representative of power utilities and member of the Energy Sector SCC, stated that public and private sector officials agreed that there were not operational impacts caused by the malicious cyber activity [73].

US-CERT noted that Russian cyber activity crossed several sectors of critical infrastructure [45]. The malicious cyber activity centered around business networks of plants categorized as being within the Energy, Commercial Facilities, and Critical Manufacturing Sectors, among others. After gaining access to business networks, the cyber actors would pivot into systems that received data from or contained information on the plant's ICS and SCADA systems. The alerts from US-CERT were the result of collaboration between DHS and FBI and their work with infrastructure owners and operators. DHS and the FBI recommended that network administrators review and apply mitigations published in the alerts and technical reports.

In March 2018, the same month the US-CERT alert was released, the DoE released the Multiyear Program Plan for Energy Sector Cybersecurity [74]. The plan states that the DoE established a dedicated office to lead cybersecurity efforts across the Energy Sector in alignment with DoE's sector-specific agency roles and responsibilities. The goals outlined in the plan are strengthened cybersecurity, coordinated incident response, and accelerated research and development. These goals align with sector-specific agency goals described in the sector-specific plan. Related to the sector-specific plan, the cybersecurity plan expounds on the cyber threats and financial impacts of cyber crime to the Energy Sector in comparison to other critical infrastructure sectors. The development of a dedicated DoE office to promote cybersecurity is the notable accomplishment presented in the plan.

In November 2017, The Energy Sector held the fourth iteration of a semiannual exercise on response and recovery to physical and cyber threats [75]. The goal of the

exercise was to minimize effects of emergency power disruptions and identify weaknesses in coordination efforts across the sector. A noted measure of success in the exercise was the increased participation. The coordination channels used during the exercise were the same as those described in the sector-specific plan, such as using the sector's ISAC for technical assistance. The exercise and sector-specific plan place emphasis on the sector's resilience in the face of major power disruptions.

The more recent cybersecurity plan developed by DoE reinforces the reliance on private sector participation to strengthen sector security and resilience. The plan also shifts focus towards the prevention of cyber incidents, as opposed to recovery operations in the event of power disruption. The plan's focus on preventing cyber incidents is likely needed to promote security across the sector, following the Russian malicious cyber activity.

C. IRANIAN DISTRIBUTED DENIAL OF SERVICE ATTACKS AGAINST FINANCIAL INSTITUTIONS

Operation Ababil, as it was named by the perpetrators, was a series of denial of service cyber attacks against U.S. financial institutions in late 2012 [50]. The attacks were conducted by Iranian cyber actors, most likely sponsored by the Iranian government. The attacks lasted for months, beginning one week after physical protests and attacks against U.S. embassies, consulates, and diplomatic outposts in locations such as Yemen, Tunisia, and Libya. U.S. cybersecurity firm Recorded Futures noted that the protests may have been used as cover by the cyber actors to portray the attacks as hacktivism rather than as Iranian state-sponsored acts as U.S. government officials asserted [76].

According to analysis by various cybersecurity firms, the cyber attacks against U.S. financial institutions were part of a broader campaign that involved minor, sporadic attacks beginning in 2011 and culminated in a series of more significant, coordinated distributed denial of service (DDoS) attacks against small and large financial institutions, to include the New York Stock Exchange and J.P Morgan Chase [77]. These cyber attacks affected at least 46 major financial institutions over at least 176 days and may have resulted in the loss of tens of millions of dollars in revenue [76]. As a result of the attacks, a U.S. grand jury brought charges against several Iranian cyber actors [78].

The sector-specific plan specifies that cyber attacks, like the ones carried out by Iranian cyber actors, highlight the need for partnership structures described in the NIPP and coordination with DHS, law enforcement agencies, the NCCIC, the sector's ISAC, and others. The plan also stresses the need for rapid information sharing and continued utilization of the NIST Cybersecurity Framework. The required partnerships, the NCCIC, and the ISAC existed prior to the sector-specific plan, though some organizations have subsequently changed names. Prescribed utilization of the NIST Cybersecurity Framework [12] and the establishment of the Financial Services Sector Cyber Intelligence Group are notable changes to the status quo described in the plan.

The NIST Cybersecurity Framework is a standardized approach to cybersecurity and the Cyber Intelligence Group is a Financial Services Sector information sharing center. Standardized cybersecurity practices and more efficient information sharing likely enhance critical infrastructure security, however it is unlikely either implementation of the framework or establishment of the Cyber Intelligence Group would have prevented the Iranian cyber attack. Rather, it is likely that the impact of the cyber attacks could have been reduced and that the duration could have been shortened.

D. CHINESE EXFILTRATION OF DATA

In 2014, a grand jury indicted five Chinese cyber actors for cyber attacks against various U.S. industries [79]. The indictment followed the publication of a report by the cybersecurity firm Mandiant detailing the activities of an advanced persistent threat referred to in the report as APT-1 [80]. While it is important to note that the indictments were a result of U.S. government intelligence and law enforcement operations, the report does provide independent corroboration of the government's assertions. In particular, the report asserts that APT-1 was directly associated with a unit of the People's Liberation Army. Further, the report characterized the activity as an extensive state-sponsored cyber operation against the U.S. private sector.

The extent of cyber attacks by China against the U.S. was not limited to a specific period nor was it directed against a single segment of U.S. infrastructure. Rather, more recent activity attributed to state-sponsored Chinese actors, such as a cyber attack against

a U.S. Navy contractor in 2018, has also been observed [81]. This particular attack involved the exfiltration of over 600 gigabytes of sensitive information related to undersea warfare. A more general assessment of Chinese state-sponsored cyber operations against the U.S. was disseminated in the Worldwide Threat Assessment of the U.S. Intelligence Community, provided by the Director of National Intelligence in 2018 [82]. The report detailed the following activity by China:

> China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities. The IC and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015. Most detected Chinese cyber operations against U.S. private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015. [82]

The campaign of malicious cyber activity by Chinese cyber actors detailed in the Mandiant report and elsewhere addresses a threat to U.S. industry but does not directly reference critical infrastructure. Nevertheless, it clearly impacts multiple sectors. PPD-21 directs DOD and the intelligence community to contribute to the NCIJTF in order to provide threat intelligence to DHS. DOD's Cyber Strategy expands on the limited role directed in PPD-21. Per the strategy, DOD focuses on foreign threats, then works with other federal departments to defend the critical infrastructure to which the threat applies. DOD defense efforts are focused on providing indications and warning to DHS and other federal agencies and on stopping cyber attacks at a potential point of origin on foreign adversarial networks or intermediate networks through which the attacks are conducted. DOD provides cyber threat information to the DHS-led NCIJTF who is then in a position to share it with sector-specific agencies and other federal cyber centers. The sector-specific categorization of critical infrastructure does not inhibit the security and resilience of critical infrastructure from threats and attacks that span multiple sectors, such as the case of Chinese cyber actors that threaten U.S. industries.

E. SUMMARY

In each described cyber attack, the three lines of effort prescribed in PPD-41 were effectively executed. Threat response was carried out by DoJ and the FBI, and specific actors were identified and named in each case. Asset response was performed by CISA and resulted in the development and promulgation of mitigations, often through US-CERT alerts. Finally, intelligence and support activities, the third line of effort, were effectively conducted and information was disseminated to stakeholders as required. U.S. Cyber Command assistance in malware analysis in support of attribution efforts following the cyber attack against Sony provides one example.

The criteria each sector is assessed by in Chapter III can be reasonably determined to characterize the readiness of the sector-specific agencies and address a cyber attack. Before the attack against Sony, for instance, the Commercial Facilities Sector Cyber Working Group promoted the NIST Cybersecurity Framework, identified critical cybersecurity functions and services in accordance with Executive Order 13636, and worked with sector partners and subject matter experts to set cyber risk priorities [16]. That the assessment that the Commercial Facilities Sector was evaluated as adequately organized to implement cybersecurity measures does not imply that a targeted attack by a nation-state adversary will not occur or that it will not have effects. Rather, it assessed the readiness of the sector to respond to the cyber incidents to minimize their effects.

In the case of Russian infiltration into the Energy Sector, the institutional knowledge of DoE continues to enhance security of the sector, though it did not stop the infiltration. DoE and sector partners appropriately qualified the threat, noting there was no operational impact. DoE continues to refine sector cybersecurity practices through its cybersecurity plan and ongoing exercises that focus on security in addition to resiliency. Evidently, there is continuity of efforts by DoE to enhance sector security, in the face of an advanced threat.

In the case of the Financial Services cyber attacks by Iranian cyber actors, the sector-specific plan implemented security measures based on lessons learned from the attacks. It is reasonably expected that the Cyber Intelligence Group, as an information

sharing center, can reduce both the duration and number of institutions affected by similar cyber attacks in the future. Again, while it is unlikely a targeted attack of this sort by an advanced adversary can be altogether prevented, effective execution of the sector-specific plan can significantly improve the response.

The sector-specific plans describe continuing efforts within the sectors to enhance information sharing and response actions, and it is likely that those efforts will also reduce the negative effects of future cyber attacks. Broad implementation of the Cybersecurity Framework, timely dissemination of mitigations, and rapid response can also be reasonably expected to reduce the duration of an attack, its overall effectiveness, and its spread across infrastructure. Cyber attacks that threaten national security, such as the prolific data exfiltration campaign by Chinese cyber actors, are not necessarily confined to a single category of critical infrastructure or may extend beyond what is considered critical infrastructure. Though the sector-based approach to protecting critical infrastructure is adequate, the more recent addition of a functions-based risk management approach described in Chapter II enhances cybersecurity of critical infrastructure across sector boundaries. For example, U.S. Cyber Command conducts operations in support of prioritized efforts to defend elections and election infrastructure [83]. This example represents prioritized cybersecurity efforts, based on the NRMC functions-based approach.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

The PPD-21 prescribed sector-based approach to critical infrastructure constrains the cybersecurity efforts. This thesis utilized three criteria derived from PPD-21 to assess the sector-based approach: expertise or a notable advantage of the sector-specific agency; promotion of cybersecurity measures by the partnership structure; and legislation, policy, or sector-specific characteristics that enhance security and resilience of the sector. Supporting policy and organizational structures present the basis for the assessment. Cyber attacks against critical infrastructure are described and demonstrate limitations of the sector-based approach.

Chapter I introduces national policy that directs the government to strengthen the security and resilience of critical infrastructure. The national policy defines the sector-based approach to critical infrastructure and directs the federal effort to protect critical infrastructure and respond to cyber incidents. Importantly, national policy assigns primary responsibility for critical infrastructure security to DHS and supporting roles and responsibilities to additional federal departments and agencies.

As it relates to critical infrastructure security, Chapter II examines the assigned tasks of national policy, the DHS organization, and the National Infrastructure Protection Plan. The NIPP standardizes the sector-based approach by defining partnership structures, establishing a risk management process, and promoting the NIST Cybersecurity Framework. The public-private partnership structure supports the national unity of effort directed by PPD-21. The NIST Cybersecurity Framework was developed for broad use and implementation across critical infrastructure. The CISA and the NRMC are components of DHS responsible for critical infrastructure protection.

Chapter III assesses each sector of critical infrastructure, compares sector-specific agencies, and examines sector-specific legislation. There are noted strengths and deficiencies in sectors. Several sectors are assessed as well organized to implement cybersecurity measures, though several are assessed as inadequately organized.

Chapter IV demonstrates limitations of the sector-based approach through examination of cyber attacks against critical infrastructure. Though, organizational structures and incident responses are assessed to reasonably reduce effects of cyber attacks, nation-state adversaries are capable of successful, targeted attacks against critical infrastructure.

National policy directs the protection of critical infrastructure against cyber threats. Executive Order 13636, Improving Critical Infrastructure Cybersecurity, states the following:

> The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards. [13]

Public and private sector partnerships are well defined in the NIPP and adequately organized by the sector-based approach to critical infrastructure security. In accordance with Executive Order 13636, the NIST Cybersecurity Framework is promoted across public and private sector by the partnership structure. In some instances, public and private collaboration led to development of tailored versions of the Cybersecurity Framework, based upon sector-specific characteristics. These tailored versions of the Cybersecurity Framework are examples of the partnership structure's effectiveness in implementing cybersecurity measures in support of the sector-based approach.

This thesis assesses the sector-based approach as adequately structured to implement cybersecurity measures and defend critical infrastructure from cyber threats. Initially, the scope and scale of critical infrastructure indicated an untenable challenge to implementation of cybersecurity measures across critical infrastructure. Public-private partnerships and the federal roles and responsibilities support national policy that directs

strengthening of critical infrastructure security and resilience. The scope and scale of critical infrastructure is inconsequential to security efforts. The sector-based approach supports broad implementation of cybersecurity measures.

For continual evaluation of government's effectiveness in protecting critical infrastructure, additional study of the intersection of the functions-based risk management approach by the NRMC and the sector-specific approach will complement the assessments in Chapter III. There are indications of a positive intersection between the two, as evidenced by the efforts of government to protect U.S. elections. National Critical Functions may answer the question posed by ADM Rogers (ret.) about reconsidering the sector-based approach to critical infrastructure. Furthermore, focused analysis of any critical infrastructure sector's cybersecurity efforts may determine sector-specific limitations or strengths to the sector-specific approach.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] *Critical Infrastructure Security and Resilience*, Presidential Policy Directive 21, White House, Washington, DC, USA, 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidentialpolicy-directive-critical-infrastructure-security-and-resil.

[2] United States Cyber Incident Coordination, Presidential Policy Directive 41, White House, Washington, DC, USA, 2016. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidentialpolicy-directive-united-states-cyber-incident.

[3] Department of Homeland Security, "National Cyber Incident Response Plan," Washington, DC, USA, 2016. [Online]. Available: https://www.uscert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[4] Department of Homeland Security, "Cybersecurity Strategy," Washington, DC, USA, 2019. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/DHS-CybersecurityStrategy_1.pdf.

[5] Department of Defense, "Cyber Strategy," Washington, DC, USA 2018. [Online]. Available: https://media.defense.gov/2018/Sep/18/2002041658/-1/- 1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[6] Department of Homeland Security, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," Washington, DC, USA, 2013. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nationalinfrastructure-protection-plan-2013-508.pdf.

[7] Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Partnership Advisory Council," August 12, 2020. [Online]. Available: https://www.cisa.gov/critical-infrastructure-partnership-advisory-council.

[8] Cybersecurity and Infrastructure Security Agency, "Sector Coordinating Councils," December 4, 2018. [Online]. Available: https://www.cisa.gov/sectorcoordinating-councils.

[9] Cybersecurity and Infrastructure Security Agency, "Government Coordinating Councils," December 4, 2018. [Online]. Available: https://www.cisa.gov/government-coordinating-councils.

[10] National Council of ISACs, "National Council of ISACs." Accessed July 19, 2020. [Online]. Available: https://www.nationalisacs.org.

[11] Cybersecurity and Information Security Agency, Joint National Priorities, 2018. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/ JointNational-Priorities-Fact-Sheet-20180928-508.pdf.

[12] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Washington, DC, USA, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[13] *Improving Critical Infrastructure Cybersecurity*, Executive Order 13636, White House, Washington, DC, USA, 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/ executiveorder-improving-critical-infrastructure-cybersecurity.

[14] Department of Homeland Security, “Critical Infrastructure Security,” July 14, 2020. [Online]. Available: https://www.dhs.gov/topic/critical-infrastructuresecurity.

[15] *Removal of Kaspersky-branded Products*, Binding Operational Directive 17–01, Acting Secretary of Homeland Security, Washington, DC, 2017. [Online]. Available: https://cyber.dhs.gov/assets/report/bod-17-01.pdf.

[16] Cybersecurity and Infrastructure Security Agency, “National Infrastructure Coordinating Center.” November 21, 2018. [Online]. Available: https://www.cisa.gov/national-infrastructure-coordinating-center.

[17] Cybersecurity and Infrastructure Security Agency, “National Cybersecurity Communications Integration Center.” Accessed: July 19, 2020. [Online]. Available: https://www.cisa.gov/national-cybersecurity-communicationsintegration-center.

[18] Cybersecurity and Infrastructure Security Agency, “National Critical Functions Overview,” January 13, 2020. [Online]. Available: https://www.cisa.gov/ nationalcritical-functions-overview.

[19] Cybersecurity and Infrastructure Security Agency, “NRMC,” March 19, 2020. [Online]. Available: https://www.cisa.gov/nrmc.

[20] “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” *The White House*. https://www.whitehouse.gov/presidential-actions/presidential-executive-orderstrengthening-cybersecurity-federal-networks-critical-infrastructure/ (accessed Jul. 19, 2020).

[21] Cybersecurity and Infrastructure Security Agency, “CISA Insights,” June 15, 2020. [Online]. Available: https://www.cisa.gov/insights.

[22] M. S. Rogers, “Cybersecurity Threats: The Way Forward,” presented at House Permanent Select Committee on Intelligence, Washington, DC, USA, Nov. 20, 2014. [Online]. Available: https://www.nsa.gov/public_info/_files/ speeches_testimonies/ADM.ROGERS.Hil l.20.Nov.pdf.

[23] M. S. Rogers, “Fiscal Year 2019 Cyber Command Budget Request,” presented at House Subcommittee on Intelligence and Emerging Threats and Capabilities, Washington, DC, USA, Mar. 13, 2019. [Online]. Available: https://armedservices.house.gov/2019/3/fiscal-year-2020-budget-request-for-u-scyber-command-and-operations-in-cyberspace.

[24] D. Riedman, “Questioning the Criticality of Critical Infrastructure: A Case Study Analysis,” *Homel. Secur. Aff.*, vol. XVI, May 2016, Accessed: Nov. 30, 2019. [Online]. Available: https://www.hsaj.org/articles/10578.

[25] Federal Cybersecurity Center, ”Cyber Incident Severity Schema.” Accessed: Nov. 30, 2019. [Online]. Available: https://obamawhitehouse.archives.gov/sites/ whitehouse.gov/files/documents/Cybe r%2BIncident%2BSeverity%2BSchema.pdf.

[26] Department of Homeland Security, “Chemical Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/ default/files/publications/nipp-ssp-chemical-2015- 508.pdf.

[27] Cybersecurity and Infrastructure Security Agency, “Chemical Sector,” March 24, 2020. [Online]. Available: https://www.cisa.gov/chemical-sector.

[28] F. Shannon, “Chemical Security Analysis Center,” July 16, 2019. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/2019-csss-csacoverview-508.pdf.

[29] American Chemistry Council, “Cyber.” Accessed November 30, 2019. [Online]. Available: https://www.americanchemistry.com/Cybersecurity/.

[30] American Chemistry Council, “President’s Executive Order 13650 – Improving Chemical Facility Safety and Security, Accessed November 30, 2019. [Online] https://www.americanchemistry.com/Policy_Pages/Security_and_Safety/Presiden t_s_Executive_Order_13650_– _Improving_Chemical_Facility_Safety_and_Security/.

[31] Department of Homeland Security, “Chemical Facility Anti-Terrorism Standards,” Washington, DC, USA, 2009. [Online]. Available: https://www.dhs.gov/cisa/chemical-facility-anti-terrorism-standards.

[32] Department of Homeland Security, “Commercial Facilities Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/ default/files/publications/nipp-ssp-commercialfacilities-2015-508.pdf.

[33] N. Rasmussen, Director, National Counterterrorism Center, “Current Terrorist Threat to the United States,” hearing before Senate Select Committee on Intelligence, Washington, DC, USA, Feb. 12, 2015. [Online] Available: https://www.dni.gov/index.php/newsroom/congressionaltestimonies/congressional-testimonies-2015/item/1173-national-counterterrorismcenter-director-nicholas-j-rasmussen-statement-for-the-record-before-the-ssci.

[34] Department of Homeland Security, “Communications Sector-Specific Plan,” Washington, DC, USA 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-communications2015-508.pdf.

[35] Assignment of National Security and Emergency Preparedness Communications Functions, Executive Order 13618, White House, Washington, DC, USA, 2012. [Online] Available: https://obamawhitehouse.archives.gov/the-pressoffice/2012/07/06/executive-order-assignment-national-security-and-emergencypreparedness-.

[36] Department of Homeland Security, “Critical Manufacturing Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-criticalmanufacturing-2015-508.pdf.

[37] Cybersecurity and Infrastructure Security Agency, “HIDDEN COBRA – North Korea’s DDoS Botnet Infrastructure.” Accessed: November 30, 2019. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-164A.

[38] Cybersecurity and Infrastructure Security Agency, “Multiple Petya Ransomware Infections Reported,” July 16, 2017. [Online]. Available: https://www.uscert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-RansomwareInfections-Reported.

[39] Cybersecurity and Infrastructure Security Agency, “Dams Sector,” December 4, 2018. [Online]. Available: https://www.dhs.gov/cisa/dams-sector.

[40] Department of Homeland Security, “Dams Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-dams-2015-508.pdf.

[41] Cybersecurity and Infrastructure Security Agency, “Dams Sector Cybersecurity Framework Implementation Guidance.” Washington, DC, USA, May 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Dams_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf.

[42] Department of Defense, “Defense Industrial Base Sector-Specific Plan,” Washington, DC, USA, 2010. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf.

[43] Department of Homeland Security, “Emergency Services Sector Profile,” Washington, DC, USA, 2017. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/NPPD_emergency-servicessector-profile-v3.pdf.

[44] Cybersecurity and Infrastructure Security Agency, “Energy Sector-Specific Plan,” December 4, 2018. [Online]. Available: https://www.dhs.gov/cisa/energy-sector.

[45] Cybersecurity and Infrastructure Security Agency, “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” Accessed: November 30, 2019. [Online]. Available: https://www.uscert.gov/ncas/alerts/TA18-074A.

[46] Dragos, “Crashoverride: Threat to Electric Grid Operations,” Accessed November 30, 2019. [Online]. Available: https://dragos.com/wpcontent/uploads/CrashOverride-01.pdf.

[47] Axios, “Why ‘Crashing the Grid’ Doesn’t Keep Cyber Experts Awake at Night.” Accessed: December 1, 2019. [Online]. Available: https://www.axios.com/whycrashing-the-grid-doesnt-keep-cyber-experts-awake-at-night-a40563a5-f266-493d-856a-5c9a5c1383dd.html.

[48] Idaho National Laboratory, “Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector,,” Idaho Falls, ID, USA, Mission Support Center Analysis Report, August 2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

[49] National Risk Management Center, “Pipeline Cybersecurity Initiative,” July 13, 2020. [Online]. Available: https://www.dhs.gov/cisa/pipeline-cybersecurityinitiative.

[50] Department of the Treasury, “Financial Services Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services2015-508.pdf.

[51] Department of Agriculture & Department of Health and Human Services, “Food and Agriculture Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-food-ag2015-508.pdf.

[52] Department of Homeland Security & General Services Administration, “Government Facilities Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nippssp-government-facilities-2015-508.pdf.

[53] United States Senate, “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election,” Washington, DC, USA, Select Committee on Intelligence Report, Vol. I, 2016. [Online]. Available: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

[54] Department of Health and Human Services, “Healthcare and Public Health Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-publichealth-2015-508.pdf.

[55] Department of Health and Human Services, “Critical Infrastructure Protection for the Healthcare and Public Health Sectors,” May 13, 2020. [Online]. Available: http://www.phe.gov/preparedness/planning/cip/Pages/default.aspx.

[56] Health and Human Services, “FY 2020 Budget & Performance,” February 20, 2020. [Online]. Available: https://www.hhs.gov/about/budget/index.html.

[57] Department of Homeland Security, “Information Technology Sector-Specific Plan,” Washington, DC, USA, 2016. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-informationtechnology-2016-508.pdf.

[58] Department of Homeland Security, “Nuclear Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015- 508.pdf.

[59] Cybersecurity and Infrastructure Security Agency, “Nuclear Reactors, Materials, and Waste Sector,” December 11, 2019. [Online]. Available: https://www.cisa.gov/nuclear-reactors-materials-and-waste-sector.

[60] Department of Homeland Security, “Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nuclear-cybersecurityframework-implementation-guide-2015-508.pdf.

[61] Department of Transportation, “Transportation Systems Sector-Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportationsystems-2015-508.pdf.

[62] Senate Committee on Energy and Natural Resources, “Cantwell, Pallone Demand Immediate Action On Pipeline Cybersecurity From DHS.” December 19, 2018. [Online]. Available: https://www.energy.senate.gov/public/index.cfm/2018/12/cantwell-pallonedemand-immediate-action-on-pipeline-cybersecurity-from-dhs.

[63] Government Accountability Office, “Critical Infrastructure Protection,” Washington, DC, USA, GAO Report No. GAO-19-48, 2018. [Online]. Available: https://www.gao.gov/assets/700/696123.pdf.

[64] Environmental Protection Agency, “Water and Wastewater Systems Sector Specific Plan,” Washington, DC, USA, 2015. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

[65] Environmental Protection Agency, “Water Infrastructure Resilience,” Accessed December 1, 2019. [Online]. Available: https://www.epa.gov/homeland-securityresearch/water-infrastructure-resilience.

[66] Environmental Protection Agency, “Water Sector Cybersecurity Brief for States,” June 2018. [Online]. Available: https://www.epa.gov/sites/production/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf.

[67] Government Accountability Office, “Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress,” Washington, DC, USA, GAO Report No. GAO-12-296, 2013. [Online]. Available: https://www.hsdl.org/?view&did=733365.

[68] Cybersecurity and Infrastructure Security Agency, “About CISA,” Accessed November 30, 2019. [Online]. Available: https://www.cisa.gov/about-cisa.

[69] Department of Homeland Security, “Organizational Chart,” Accessed November 30, 2019. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/19_0628_dhs-organizationalchart.pdf.

[70] C. Bennett, interview, December 2014. [Online]. Available: https://www.cspan.org/video/?323103-4/washington-journal-cory-bennett-hacking-cyberthreats.

[71] R. Faughnder, “Sony says studio hack cost it $15 million in fiscal third quarter,” L.A. Times, February 4, 2015. [Online]. Available: https://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-cost20150204-story.html.

[72] Cybersecurity and Infrastructure Security Agency, “Alert AA20-106A: Guidance on the North Korean Cyber Threat.” Jun. 23, 2020. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-106a.

[73] American Public Power Association, “DHS holds briefings on Russian cyber threats to power grid,” Accessed November 30, 2019. [Online]. Available: https://www.publicpower.org/periodical/article/dhs-holds-briefings-russian-cyberthreats-power-grid).

[74] Department of Energy, “Multiyear Plan for Energy Sector Cybersecurity,” Washington, DC, USA, Mar. 2018. [Online]. Available: https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

[75] American Public Power Association, “North American exercise focused on cyber, physical threats to the grid,” December 4, 2017. [Online]. Available: https://www.publicpower.org/blog/north-american-exercise-focused-cyber-physical-threats-grid.

[76] Recorded Future, “Deconstructing the Al-Qassam Cyber Fighters Assault on U.S. Banks,” January 02, 2013. [Online]. Available: https://www.recordedfuture.com/deconstructing-the-al-qassam-cyber-fightersassault-on-us-banks/.

[77] Carnegie Endowment for International Peace, “Timeline of Cyber Incidents Involving Financial Institutions.” Accessed: Nov. 30, 2019. [Online]. Available: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

[78] District Court Southern District of New York. Sealed Indictment, United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, a/k/a “Nitr0jen26,” Omid Ghaffarinia, a/k/a “PLuS,” Sina Keissar, and Nader Saedi, a/k/a “Turk Server. [Online]. Available: https://www.justice.gov/opa/file/834996/download.

[79] Department of Justice, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” May 19, 2014. [Online]. Available: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyberespionage-against-us-corporations-and-labor.

[80] Mandiant, “APT1: Exposing One of China’s Cyber Espionage Units” Milpitas, CA, USA, 2013. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1- report.pdf.

[81] E. Nakashima & P. Sonne, “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare,” *Washington Post*, Jun. 8, 2018. [Online]. Available: https://www.washingtonpost.com/world/nationalsecurity/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitivedata-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

[82] D. Coats, “Worldwide Threat Assessment of the U.S. Intelligence Community,” Director of National Intelligence, Statement for the Record, Feb. 13, 2018. [Online]. Available: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA--- Unclassified-SSCI.pdf.

[83] C. Todd Lopez, “Cyber Command Expects Lessons From 2018 Midterms to Apply in 2020,” *Defense.gov*, Feb. 14, 2019. [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/1758488/cyber-commandexpects-lessons-from-2018-midterms-to-apply-in-2020/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California